Kaspersky Endpoint Security 8 for Smartphone

pour Microsoft® Windows® Mobile OS

Guide de l'utilisateur

VERSION DE L'APPLICATION : 8.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que cette documentation vous sera utile dans votre travail et vous apportera toutes les réponses sur notre produit logiciel.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément aux lois de la France.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et ses illustrations ne peuvent être utilisés qu'à des fins d'information à usage non-commercial ou personnel.

Ce document peut être modifié sans préavis. Pour obtenir la dernière version de ce document, reportez-vous au site de Kaspersky Lab à l'adresse http://www.kaspersky.com/fr/docs.

Kaspersky Lab décline toute responsabilité en rapport au contenu, à la qualité, à la pertinence ou à la précision de matériels, utilisés dans ce document, dont les droits sont la propriété de tiers, ou aux dommages potentiels associés à l'utilisation de ce type de documents.

Ce document fait référence à des marques enregistrées et à des marques de services qui appartiennent à leurs propriétaires respectifs.

Date d'édition : 27.05.2011

© Kaspersky Lab ZAO, 1997–2011

http://www.kaspersky.com/fr
http://support.kaspersky.fr/

TABLE DES MATIERES

A PROPOS DE CE MANUEL

Le présent document est un Guide d'installation, de configuration et d'utilisation de l'application Kaspersky Endpoint Security 8 for Smartphone. Ce document est destiné au grand public.

Buts du document :

- aider l'utilisateur à installer l'application sur l'appareil mobile par ses propres soins, à l'activer et à configurer l'application d'une manière équilibrée en fonction des tâches utilisateur ;
- à assurer une recherche d'information rapide pour résoudre des problèmes liés à l'application ;
- à informer sur les autres sources d'information concernant l'application, ainsi que sur les possibilités d'obtenir l'assistance technique.

SOURCES D'INFORMATIONS COMPLEMENTAIRES

Pour toute question sur l'installation ou l'utilisation de Kaspersky Endpoint Security 8 for Smartphone, vous pouvez rapidement trouver des réponses en utilisant plusieurs sources d'information. Vous pouvez sélectionner celle qui vous convient le mieux en fonction de l'importance et de l'urgence du problème.

DANS CETTE SECTION

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur le programme :

- la page de l'application sur le site de Kaspersky Lab ;
- page du logiciel, sur le site du serveur du Support technique (Base de connaissances) ;
- système d'aide en ligne ;
- documentation.

Page sur le site Web de Kaspersky Lab

http://www.kaspersky.com/fr/endpoint-security-smartphone

Utilisez cette page pour obtenir des informations générales sur Kaspersky Endpoint Security 8 for Smartphone, ses possibilités et ses caractéristiques de fonctionnement.

Page de l'application sur le serveur du Support technique (Base de connaissances)

http://support.kaspersky.com/fr/kes8m

Cette page contient des articles publiés par les experts du Service d'assistance technique.

Ils contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de Kaspersky Endpoint Security 8 for Smartphone. Ces articles sont regroupés par sujet, par exemple «Utilisation des fichiers de licence», «Mise à jour des bases» ou «Elimination des échecs». Les articles répondent non seulement à des questions sur Kaspersky Endpoint Security 8 for Smartphone, mais aussi sur d'autres produits Kaspersky Lab ; ils peuvent contenir des informations générales récentes du Service d'assistance technique.

Système d'aide en ligne

En cas de problème concernant un écran ou un onglet spécifiques de Kaspersky Endpoint Security 8 for Smartphone, vous disposez de l'aide contextuelle.

Pour accéder à l'aide contextuelle, ouvrez l'écran en question et cliquez sur **Aide** ou sélectionnez **Menu** → **Aide**.

Documentation

Le kit de distribution de Kaspersky Endpoint Security 8 for Smartphone comprend **Guide de l'utilisateur** (format PDF). Ce document décrit les procédures d'installation, de suppression, d'administration des paramètres de l'application, ainsi que celles de premier lancement de l'application et de configuration de ses composants. Le

document décrit l'interface de l'application, propose des solutions pour des tâches type de l'utilisateur lors de l'utilisation de l'application.

PUBLIER DES MESSAGES DANS LE FORUM SUR LES APPLICATIONS DE KASPERSKY LAB

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.com.

Le forum permet de lire les conversations existantes, d'ajouter des commentaires, de créer de nouvelles rubriques et il dispose d'une fonction de recherche.

CONTACTER L'EQUIPE DE REDACTION DE LA DOCUMENTATION

Si vous avez des questions concernant la documentation, ou vous y avez trouvé une erreur, ou vous voulez laisser un commentaire sur nos documents, vous pouvez contacter les spécialistes du Groupe de rédaction de la documentation pour les utilisateurs. Pour contacter l'Équipe de rédaction de la documentation, envoyez un message à docfeedback@kaspersky.com. Dans le champ d'objet mettez «Kaspersky Help Feedback : Kaspersky Endpoint Security 8 for Smartphone».

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone protège les appareils mobiles tournant sous Microsoft® Windows® Mobile. L'application protège les données de l'appareil contre l'infection par des menaces connues, refuse les SMS et les appels non sollicités, contrôle les connexions de réseau de l'appareil, chiffre les données, masque les informations pour les contacts confidentiels et protège les données confidentielles en cas de perte ou de vol de l'appareil. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier. L'installation et la configuration de l'application sont effectuées par l'administrateur via les systèmes d'administration distante.

Kaspersky Endpoint Security 8 for Smartphone reprend les composants de protection suivants :

- **Anti-Virus**. Protège le système de fichiers de l'appareil mobile contre les virus et autres programmes malveillants. Antivirus permet d'identifier et de neutraliser les objets malveillants sur votre appareil, ainsi que de mettre à jour les bases antivirus de l'application.
- **Anti-Spam**. Analyse tous les SMS et appels entrants à la recherche de spam. Le composant permet de configurer en souplesse la fonction de blocage des SMS et des appels considérés comme indésirables.
- **Antivol** Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol tout en facilitant sa recherche. Antivol permet de verrouiller l'appareil à distance à l'aide des SMS, de supprimer les données qu'il contient et de déterminer ses coordonnées géographiques (si l'appareil mobile est doté d'un récepteur GPS). De plus, Antivol permet également de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.
- **Contacts personnels**. Masque les informations liées aux numéros confidentiels de la Liste des contacts que vous avez créée. Les Contacts personnels masquent les entrées des Contacts, les SMS, les entrées dans le journal des appels, les SMS reçus et les appels entrants pour ce type de numéros.
- **Pare-feu**. Contrôle les connexions de réseau de votre appareil mobile. Le Pare-feu permet de définir les connexions qui seront autorisées ou interdites.
- **Chiffrement**. Stocke les données en mode crypté. Le composant Chiffrement permet de crypter un nombre quelconque de dossiers qui ne sont pas définis par le système et enregistrés aussi bien dans la mémoire de l'appareil que sur les cartes mémoire. L'accès aux fichiers depuis les dossiers chiffrés est offert uniquement après avoir saisi le code secret de l'application.

Outre cela, l'application propose diverses fonctions de service permettant de maintenir l'application dans un état actuel, élargir les possibilités d'utilisation de l'application, et ceux qui aide l'utilisateur à travailler :

- État de la protection. Les états des composants de l'application sont affichés. Les informations proposées permettent d'évaluer l'état actuel de la protection des données stockées sur l'appareil.
- La mise à jour des bases antivirus de l'application. Cette fonction permet de maintenir les bases antivirus de Kaspersky Endpoint Security 8 for Smartphone à jour.
- Journal des événements. Les informations sur le fonctionnement de chacun des composants (par exemple, rapport d'analyse, mise à jour des bases antivirus, détails sur un fichier bloqué) sont consignées dans un journal des événements spécifique. Les rapports sur le fonctionnement des composants sont envoyés et stockés dans le système d'administration distante.

Kaspersky Endpoint Security 8 for Smartphone ne réalise pas de copies de sauvegarde des données en vue d'une restauration ultérieure.

DANS CETTE SECTION

NOUVEAUTES DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Voici une présentation détaillée des nouveautés de Kaspersky Endpoint Security 8 for Smartphone.

Nouveautés au niveau de la protection :

- L'accès au programme est régi par un mot de passe.
- La liste des fichiers exécutables, analysés par Protection et Analyse (dans le cas de limitation du type des fichiers exécutables), est élargie. L'application analyse uniquement les fichiers exécutables des applications aux formats suivants : EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. La liste des archives analysées est également élargie. L'application analyse les archives des formats suivants : ZIP, JAR, JAD, RAR и CAB.
- Pour les contacts confidentiels, le composant Contacts personnels permet de masquer les informations suivantes : entrées dans les Contacts, correspondance SMS, journal des appels, SMS reçus et appels entrants. Les informations confidentielles sont accessibles si la fonction de dissimulation est désactivée.
- Le composant Chiffrement permet de chiffrer les dossiers enregistrés dans la mémoire de l'appareil ou sur une carte de mémoire. Le composant stocke les informations confidentielles en mode crypté et ne permet d'accéder aux informations chiffrées qu'après avoir saisi le code secret de l'application.
- La version actualisée de l'Antivol propose la fonction de Géolocalisation qui permet de recevoir les coordonnées géographiques de l'appareil au numéro de téléphone ou à l'adresse de la messagerie électronique définie en cas de perte ou de vol. De plus, Antivol propose une version actualisée de la fonction de Suppression qui permet de supprimer à distance non seulement les données personnelles de l'utilisateur, stockées dans la mémoire de l'appareil ou sur la carte mémoire, mais aussi les fichiers de la liste des dossiers à supprimer que vous avez créée.
- Pour réduire le trafic, l'application propose une nouvelle fonctionnalité qui permet de désactiver automatiquement la mise à jour des bases de l'application en itinérance.
- L'application propose également une nouvelle fonction de service Affichage des astuces : Kaspersky Endpoint Security 8 for Smartphone affiche une brève description du composant avant la configuration de ses paramètres.

CONFIGURATION LOGICIELLE ET MATERIELLE

Kaspersky Endpoint Security 8 for Smartphone peut être installé sur des appareils mobiles avec l'un des systèmes d'exploitation suivants :

- Microsoft Windows Mobile 5.0 ;
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

Certains systèmes d'administration distante ne prennent pas en charge les appareils tournés sous Microsoft Windows Mobile 5.0. Contacter l'administrateur pour préciser les systèmes d'exploitation pris en charge.

INSTALLATION DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

L'installation de Kaspersky Endpoint Security 8 for Smartphone est effectuée par l'administrateur avec des outils d'administration distante. En fonction de l'outil d'administration utilisé par l'administrateur, l'installation peut être effectuée automatiquement ou peut nécessiter une intervention de l'utilisateur.

Si l'installation de l'application nécessite une intervention de l'utilisateur, il faut recourir à une des procédures suivantes :

- L'utilitaire d'installation homonyme de l'application Kaspersky Endpoint Security 8 for Smartphone s'installe sur votre poste de travail. Il vous permet d'installer Kaspersky Endpoint Security 8 for Smartphone sur votre appareil mobile.
- Vous recevez par courrier électronique un message d'administrateur contenant la distribution de l'application ou l'instruction sur le téléchargement de la distribution. Procédez à l'installation de Kaspersky Endpoint Security 8 for Smartphone sur l'appareil mobile en vous référant aux instructions du message.

Cette section détaille les démarches qui précèdent l'installation de Kaspersky Endpoint Security 8 for Smartphone, décrit les types d'installation de l'application sur l'appareil mobile et les actions de l'utilisateur pour chacun d'eux.

DANS CETTE SECTION

INSTALLATION AUTOMATIQUE DE L'APPLICATION

L'administrateur lance l'installation de l'application sur l'appareil avec des outils d'administration distante.

L'appareil mobile reçoit la distribution de Kaspersky Endpoint Security 8 for Smartphone et exécute l'installation automatique.

Des méthodes d'installation suivantes sont prévues :

- L'application est installée sur l'appareil automatiquement sans intervention de l'utilisateur. L'état de l'installation de l'application ne sera pas affiché.
- L'application affiche l'état de l'installation. Si l'installation réussit, l'appareil affichera un message confirmant l'installation de l'application.

Le processus d'installation automatique dépend de l'outil d'administration distante que l'administrateur utilise pour installer l'application à distance.

Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

A PROPOS DE L'INSTALLATION DE L'APPLICATION VIA LE POSTE DE TRAVAIL

Si l'administrateur a installé l'utilitaire de transmission Kaspersky Endpoint Security 8 for Smartphone sur votre poste de travail, vous pouvez installer Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles connectés à cet ordinateur. L'utilitaire de transmission Kaspersky Endpoint Security 8 for Smartphone contient le distributif de l'application et le transmet sur l'appareil. Après l'installation de l'utilitaire sur le poste de travail, l'utilitaire est activé automatiquement et contrôle la connexion des appareils mobiles à l'ordinateur. A chaque connexion de l'appareil mobile au poste de travail, l'utilitaire contrôle si l'appareil est conforme aux spécifications système de Kaspersky Endpoint Security 8 for Smartphone et propose de l'installer l'application.

Pour une installation réussie, l'application Microsoft ActiveSync® doit être installée sur le poste de travail.

INSTALLATION DE L'APPLICATION VIA LE POSTE DE TRAVAIL

Si l'utilitaire de transmission Kaspersky Endpoint Security 8 for Smartphone est installé sur votre poste de travail, alors à chaque connexion des appareils, satisfaisant les exigences de système, l'installation de Kaspersky Endpoint Security 8 for Smartphone vous sera proposée.

Vous pouvez interdire l'installation de Kaspersky Endpoint Security 8 for Smartphone lors des connexions suivantes des appareils à l'ordinateur.

Pour installer l'application sur l'appareil mobile, procédez comme suit :

1. Connectez l'appareil mobile au poste de travail à l'aide de l'application Microsoft ActiveSync.
2. Si l'appareil est conforme aux spécifications système d'installation de l'application, la fenêtre **KES 8** avec les informations sur l'utilitaire s'ouvrira (cf. ill. ci-après).

Figure 1: programme d'installation de Kaspersky Endpoint Security 8 for Smartphone

3. Cliquez sur le bouton **Continuer**.

   La fenêtre **KES 8** avec la liste des appareils connectés découverts s'ouvrira.

   Si plusieurs appareils conformes aux spécifications système sont connectés au poste de travail, ils seront affichés sur la liste des appareils connectés dans la fenêtre **KES 8**.

4. Sélectionnez un ou plusieurs appareils dans la liste des appareils connectés pour installer l'application. Pour ce faire, cochez les cases à côté des appareils correspondants. (cf. ill. ci-après).

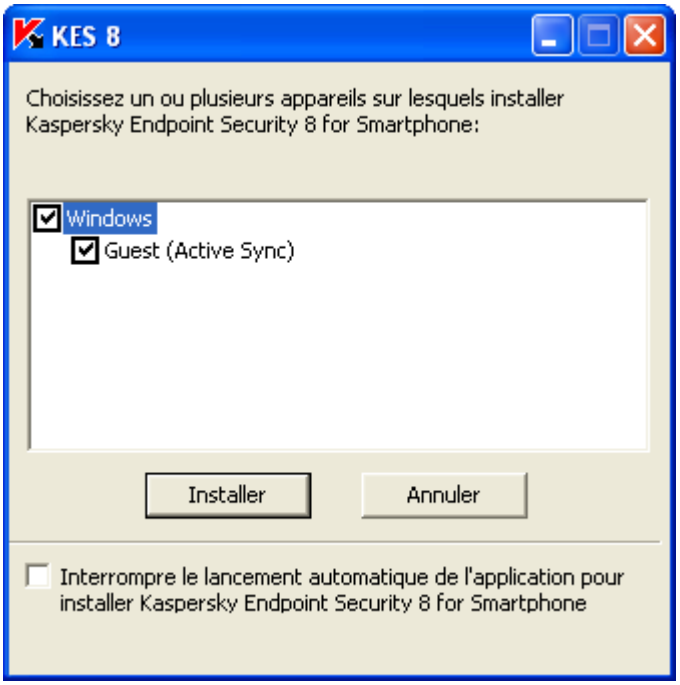

Figure 2: sélection des appareils pour installer Kaspersky Endpoint Security 8 for Smartphone

5. Cliquez sur **Installer**.

   L'utilitaire transmet la distribution de l'application vers les appareils sélectionnés. L'état de la transmission sera affiché dans la fenêtre **KES 8.0** du poste de travail.

   Après la transmission de la distribution, l'installation de l'application sur les appareils mobiles sélectionnés sera lancée automatiquement.

Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

- *Vous pouvez interdire l'installation de Kaspersky Endpoint Security 8 for Smartphone lors des connexions suivantes des appareils à l'ordinateur,*

  dans la fenêtre **KES 8**, cochez la case **Interrompre le lancement automatique de l'application pour l'installation de Kaspersky Endpoint Security 8 for Smartphone**.

A PROPOS DE L'INSTALLATION DE L'APPLICATION APRES LA RECEPTION D'UN MESSAGE ELECTRONIQUE

Vous recevez par courrier électronique un message d'administrateur contenant la distribution de l'application ou l'instruction sur le téléchargement de la distribution.

Le message contient les informations suivantes :

- la distribution de l'application jointe au message ou un lien pour la télécharger ;
- les détails sur les paramètres de connexion de l'application au système d'administration distante.

Il est déconseillé de supprimer ce message avant que Kaspersky Endpoint Security 8 for Smartphone soit installé sur l'appareil.

INSTALLATION DE L'APPLICATION APRES LA RECEPTION D'UN MESSAGE ELECTRONIQUE

Pour installer Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Ouvrez le message d'administrateur avec des paramètres d'installation de l'application depuis votre appareil mobile ou votre poste de travail.
2. Exécutez une des opérations suivantes :
   - si le message contient un lien, cliquez-le et téléchargez la distribution de l'application ;
   - si la distribution est jointe au message, téléchargez la distribution de l'application.

   Si vous téléchargez la distribution de l'application sur l'appareil mobile, elle sera enregistrée par défaut dans le dossier **Mes documents**.
3. Exécutez une des opérations suivantes :
   - si vous avez téléchargé la distribution de l'application sur l'appareil mobile, ouvrez-la ;
   - si vous avez téléchargé la distribution de l'application sur le poste de travail, connectez l'appareil mobile à l'ordinateur avec Microsoft ActiveSync, copiez la distribution sur l'appareil et ouvrez-la.

     L'installation de l'application sera effectuée automatiquement et l'application sera installée sur l'appareil.
4. Lancez l'application (cf. la rubrique «Lancement de l'application» à la page 24). Pour ce faire, sélectionnez **Démarrer** → **Programmes** → **KES 8** et lancez l'application à l'aide du stylet ou de la touche centrale du joystick.
5. Saisissez le code secret de l'application (cf. la rubrique «Installation du code secret» à la page 24). Pour ce faire, remplissez le champ **Saisissez le nouveau code**, puis le champ **Confirmation du code** et cliquez sur **OK**.

   L'écran **Paramètres de synchr.** s'ouvrira. (voir figure suivante).

Figure 3: paramètres de synchronisation

6. Spécifiez les valeurs des paramètres de connexion au système d'administration distante, s'ils figurent dans le message de l'administrateur que vous avez reçu. Saisissez les valeurs des paramètres suivant :

   - **Serveur** ;
   - **Port** ;
   - **Groupe**.

   Si la configuration des paramètres de connexion au système d'administration distante n'est pas nécessaire, cette étape est omise.

7. Saisissez l'adresse électronique de votre organisation dans le champ **Votre adresse élec.** et cliquez sur **Suivant**.

   Saisissez l'adresse électronique correctement parce qu'elle sera utilisée pour enregistrer l'appareil dans le système d'administration distante.

Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

SUPPRESSION DE L'APPLICATION

Vous pouvez supprimer l'application de l'appareil avec l'une des méthodes suivantes :

- suppression manuelle par l'utilisateur (cf. la rubrique «Suppression manuelle de l'application» à la page 16) ;
- suppression à distance effectuée par l'administrateur via le système d'administration distante.

Les actions suivantes sont automatiquement exécutées à la suppression :

- La dissimulation des informations confidentielles se désactive.
- Les données sur l'appareil qui ont été chiffrées à l'aide de Kaspersky Endpoint Security 8 for Smartphone sont déchiffrées.

Si un code secret a été saisi, pendant la suppression automatique de l'application (cf. la rubrique «Suppression automatique de l'application» à la page 17), l'utilisateur peut être amené à intervenir.

Si l'application n'a jamais été exécutée et le code secret n'a pas été saisi, la suppression automatique de l'application sera effectuée sans intervention de l'utilisateur.

DANS CETTE SECTION

SUPPRESSION MANUELLE DE L'APPLICATION

Pour supprimer l'application à la main, procédez comme suit :

1. Fermez Kaspersky Endpoint Security 8 for Smartphone. Pour ce faire, choisissez **Menu** → **Quitter**.
2. Désinstallation de Kaspersky Endpoint Security 8 for Smartphone Pour ce faire, exécutez les actions suivantes :
   a. Cliquez sur **Démarrer** → **Paramètres**.
   b. Sélectionnez **Suppr. de progr.** dans l'onglet **Système** (voir figure suivante).

*Figure 4: Onglet **Système***

c. Sélectionnez **KES 8** dans la liste des applications installées, puis cliquez sur **Supprimer**.

d. Confirmez la suppression de l'application en cliquant sur le bouton **Oui** dans la fenêtre qui s'ouvre.

e. Saisissez le code secret puis cliquez sur **OK**.

f. Indiquez s'il faut utiliser les paramètres de l'application et de l'objet pour la quarantaine :

- Pour sauvegarder la configuration de l'application ou les objets en quarantaine, appuyez sur **Enregistrer** ;
- Pour supprimer complètement une application, cliquez sur **Supprimer**.

La suppression de l'application va commencer.

Si la dissimulation des informations confidentielles sur votre appareil est activée et / ou un ou plusieurs dossiers ont été chiffrés à l'aide de Kaspersky Endpoint Security 8 for Smartphone, l'application vous invite à désactiver la dissimulation des données confidentielles et/ou à déchiffrer tous les dossiers.

3. Redémarrez l'appareil pour terminer la suppression de l'application.

SUPPRESSION AUTOMATIQUE DE L'APPLICATION

Si la suppression de l'application est effectuée par l'administrateur via le système d'administration distante et vous avez saisi le code secret de l'application, l'écran de Kaspersky Endpoint Security 8 for Smartphone s'affichera automatiquement pour vous inviter à intervenir pendant la suppression de l'application.

Pour supprimer l'application,

saisissez le code secret et cliquez sur. **OK** de l'écran de **Kaspersky Endpoint Security 8 for Smartphone**.

La fenêtre de confirmation de la suppression de l'application s'affichera. Pour confirmer la suppression de l'application, cliquez sur **Oui**.

Si la dissimulation des informations confidentielles sur votre appareil est activée et / ou un ou plusieurs dossiers ont été chiffrés à l'aide de Kaspersky Endpoint Security 8 for Smartphone, l'application vous invite à désactiver la dissimulation des données confidentielles et/ou à déchiffrer tous les dossiers.

L'application sera supprimée de l'appareil sans afficher la confirmation d'une suppression réussie.

Si vous refusez de supprimer l'application, la suppression sera annulée. Une nouvelle tentative de suppression sera faite pendant la synchronisation suivante de l'appareil avec le système d'administration distante. Ensuite, vous serez réinvité à ouvrir l'application.

ADMINISTRATION DES PARAMETRES DE L'APPLICATION

Tous les paramètres de Kaspersky Endpoint Security 8 for Smartphone, licence comprise, sont configurés par l'administrateur via le système d'administration distante. Dans ce cas, l'administrateur peut autoriser ou interdire à l'utilisateur de modifier les valeurs de ces paramètres.

Vous pouvez modifier les paramètres de fonctionnement de l'application sur l'appareil mobile si cette modification a été autorisée par l'administrateur.

L'administrateur peut interdire la modification de tous les paramètres du composant ou de certains de ses paramètres. Si en haut de l'écran de configuration du composant un verrou et un message d'avertissement s'affichent, les paramètres du composant de l'appareil mobile ne peuvent pas être modifiés.

Si l'administrateur a changé les paramètres de l'application, ils seront envoyés vers l'appareil via le système d'administration distante. Dans ce cas, les paramètres interdits à la modification par l'administrateur seront également modifiés. Les valeurs des paramètres que l'administrateur n'a pas interdit à la modification, restent les mêmes.

Si l'appareil n'a pas reçu les paramètres de l'application ou si vous voulez restaurer les valeurs des paramètres définies par l'administrateur, utilisez la fonction de la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique «Lancement de la synchronisation à la main» à la page 21).

L'utilisation de la fonction de la synchronisation n'est possible que sous la direction de l'administrateur.

GESTION DE LA LICENCE

Cette section propose des informations sur la licence, sur les modalités de son activation et la procédure de consultation des informations qui la concerne.

DANS CETTE SECTION

PRESENTATION DES LICENCES DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

La *licence* est le droit d'utilisation de Kaspersky Endpoint Security 8 for Smartphone et des services complémentaires associés offerts par Kaspersky Lab ou ses partenaires.

Pour pouvoir utiliser l'application, vous devez installer la licence.

Chaque licence se définit par sa durée de validité et son type.

La *durée de validité de la licence* désigne la période pendant laquelle vous pouvez bénéficier des services complémentaires :

- Assistance technique ;
- La mise à jour des bases antivirus de l'application.

Le volume des services proposés dépend du type de licence.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite dont la validité est limitée, par exemple 30 jours, et qui permet de découvrir Kaspersky Endpoint Security 8 for Smartphone.

  Toutes les fonctions de l'application sont accessibles pendant l'action de la version d'évaluation. Une fois la licence d'évaluation expirée, Kaspersky Endpoint Security 8 for Smartphone arrête de fonctionner. Seules les fonctions suivantes sont accessibles :

  - désactiver des composants Chiffrement et Contacts personnels ;
  - l'utilisateur peut déchiffrer les dossiers qu'il a sélectionnés pour le chiffrement ;
  - désactiver de la dissimulation des informations confidentielles ;
  - consulter le système d'aide ;
  - synchronisation avec le système d'administration distante.

- *Commerciale* : licence payante avec une durée de validité définie (par exemple, un an) octroyée à l'achat de Kaspersky Endpoint Security 8 for Smartphone.

  Toutes les fonctionnalités de l'application et les services complémentaires sont accessibles pendant la période de validité de la licence commerciale.

  Une fois que la licence commerciale a expiré, les fonctionnalités de Kaspersky Endpoint Security 8 for Smartphone seront limitées. Vous pouvez toujours utiliser les composants Anti-Spam et Pare-feu, effectuer l'analyse antivirus de votre ordinateur et utiliser les composants de la protection, mais la date de mise à jour des bases antivirus sera celle de l'expiration de la licence. Uniquement les actions suivantes sont disponibles pour d'autres composants :

  - désactiver des composants Chiffrement, Antivol et Contacts personnels ;
  - déchiffrer les dossiers sélectionnés par l'utilisateur à chiffrer ;

- désactiver de la dissimulation des informations confidentielles ;
- consulter le système d'aide ;
- synchronisation avec le système d'administration distante.

INSTALLATION D'UNE LICENCE

La licence est installée via le système d'administration distante par l'administrateur.

Toutes les fonctionnalités de Kaspersky Endpoint Security 8 for Smartphone restent opérationnelles pendant trois jours qui suivent l'installation de l'application. Durant cette période, l'administrateur installe la licence via le système d'administration distante pour activer l'application.

Si la licence n'a pas été installée pendant trois jours les fonctionnalités de l'application seront limitées. Dans ce mode vous pouvez :

- désactiver tous les composants ;
- déchiffrer un ou plusieurs dossiers ;
- désactiver de la dissimulation des informations confidentielles ;
- consulter le système d'aide.

Si la licence n'a pas été installée dans les trois jours qui suivent l'installation de l'application, pour installer la licence, utilisez la fonction de la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique «Lancement de la synchronisation à la main» à la page 21).

AFFICHAGE DES INFORMATIONS DE LICENCE

Vous pouvez consulter les informations suivantes sur la licence : le numéro de la licence, le type, la date d'activation, la date de l'expiration, le nombre de jours restant avant l'expiration et le numéro de série de l'appareil.

Pour consulter les informations sur la licence, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez **Informations** dans l'onglet.

SYNCHRONISATION AVEC LE SYSTEME D'ADMINISTRATION DISTANTE

Lors de la synchronisation, l'appareil reçois les paramètres de l'application, installés par l'administrateur. L'appareil envoie dans le système d'administration distante les rapports sur le fonctionnement des composants de l'application.

La synchronisation de l'appareil avec le système d'administration distante se fait automatiquement.

Vous pouvez toujours lancer la synchronisation à la main, si elle n'a pas été effectuée en mode automatique.

Il faut effectuer la synchronisation à la main, si dans les trois jours qui suivent l'installation de l'application la licence n'a pas été installée.

En fonction du type de système d'administration distante, sélectionné par l'administrateur pour la gestion de l'application, l'utilisateur peut être invité à saisir les paramètres de connexion au système d'administration distante pendant l'installation de l'application. Dans ce cas, les valeurs que l'utilisateur a saisi à la main peuvent être modifiées depuis l'application (cf. la rubrique «Modification des paramètres de synchronisation» à la page 22).

Il est déconseillé de modifier les paramètres de connexion au système d'administration distante sans être guidé par l'administrateur.

DANS CETTE SECTION

LANCEMENT DE LA SYNCHRONISATION A LA MAIN

Pour synchroniser l'appareil avec le système d'administration distante à la main, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez **Lancement de la synchronisation** (cf. ill. ci-après).

Figure 5: lancement manuel de la synchronisation

Si l'utilisateur n'a pas été invité à saisir les paramètres de connexion au système d'administration distante, une fenêtre de confirmation de la connexion à Internet s'affichera sur l'écran. Pour autoriser la connexion, cliquer sur **Oui**. La connexion au système d'administration distante sera établie.

Si l'utilisateur a été invité à saisir les paramètres de connexion au système d'administration distante, le système affichera l'écran **Synchronisation**. Sélectionnez l'option **Lancement de la synchronisation**. Pour autoriser la connexion à Internet, cliquer sur **Oui**. La connexion au système d'administration distante sera établie.

MODIFICATION DES PARAMETRES DE SYNCHRONISATION

Il est déconseillé de modifier les paramètres de connexion au système d'administration distante sans être guidé par l'administrateur.

Pour modifier les paramètres de connexion au système d'administration distante, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Synchronisation**.

   L'écran **Synchronisation** s'ouvre.

3. Sélectionnez l'option **Paramètres de synchronisation** (cf. ill. ci-après).

Figure 6: modification des paramètres de synchronisation

4. Modifiez les valeurs des paramètres suivants :
   - **Serveur** ;
   - **Port** ;
   - **Groupe**.
5. Appuyez sur **OK**.

PREMIERS PAS

Cette section reprend les informations sur la première utilisation de Kaspersky Endpoint Security 8 for Smartphone : la saisie du code secret de l'application, le lancement de l'application, la mise à jour des bases antivirus et l'analyse antivirus de l'appareil.

DANS CETTE SECTION

DEMARRAGE DU LOGICIEL

Pour installer Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KES 8** et démarrer le programme avec le stylo ou le bouton central du joystick.
3. Passez à la saisie du code secret de l'application (cf. rubrique «Saisie du code secret» à la page 24).

SAISIE DU CODE SECRET

Vous serez invité à saisir le code secret de l'application après son lancement. Le *code secret de l'application* permet d'éviter l'accès non autorisé aux paramètres de l'application. Vous pourrez modifier ultérieurement le code secret de l'application définit.

Kaspersky Endpoint Security 8 for Smartphone demande le code secret dans les cas suivants :

- Pour accéder à l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Géolocalisation, Contacts personnels ;
- Pour supprimer l'application.

Mémorisez le code secret de l'application. Si vous oubliez le code secret, vous ne pourrez plus gérer les fonctions de Kaspersky Endpoint Security 8 for Smartphone, ni obtenir l'accès aux fichiers chiffrés, ni supprimer l'application.

Le code secret de l'application est composé de chiffres. Le code secret doit compter au moins quatre chiffres.

Pour saisir le code secret de l'application, procédez comme suit :

1. A la première exécution de l'application, saisissez dans le champ **Saisissez le nouveau code** les chiffres qui constituent votre code.
2. Tapez de nouveau ce code dans la zone **Confirmer**.

   La robustesse du code saisi est vérifiée automatiquement.
3. Si après la vérification le code est considéré peu fiable, un message d'avertissement s'affiche sur l'écran et l'application invite l'utilisateur à confirmer la saisie. Pour utiliser le code, cliquez sur **OK**. Pour définir un nouveau code, cliquez sur **Non**.
4. A la fin, cliquez sur **OK**.

MISE A JOUR DES BASES DU PROGRAMME

Kaspersky Endpoint Security 8 for Smartphone recherche les menaces à l'aide des bases antivirus de l'application qui contiennent la description de tous les programmes malveillants connus à ce jour ainsi que les moyens de les neutraliser. On y retrouve également les descriptions d'autres objets indésirables. Il se peut que les bases antivirus livrées avec la distribution de Kaspersky Endpoint Security 8 for Smartphone, soient dépassées au moment de l'installation.

Il est conseillé d'actualiser les bases antivirus dès après l'installation de l'application.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur Internet.

Pour lancer la mise à jour des bases antivirus de l'application, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez l'option **Mise à jour**.

L'application lance la mise à jour des bases depuis le serveur défini par l'administrateur. Les informations sur la mise à jour apparaissent à l'écran.

RECHERCHE DE VIRUS SUR L'APPAREIL

Une fois l'application installée, il est conseillé de lancer l'analyse complète de l'appareil mobile à la recherche d'éventuels objets malveillants.

Vous pouvez lancer une analyse avec des paramètres actuels ou les configurer préalablement (cf. la rubrique «Analyse de l'appareil» à la page 33).

Pour lancer l'analyse complète de l'appareil, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyse**.

   L'écran **Analyse** s'ouvre.

3. Sélectionnez **Analyse complète**.

INFORMATIONS SUR LE PROGRAMME

Vous pouvez consulter les informations générales sur l'application Kaspersky Endpoint Security 8 for Smartphone et ses versions.

Pour consulter les informations sur l'application, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Infos logiciel** (cf. ill. ci-après).

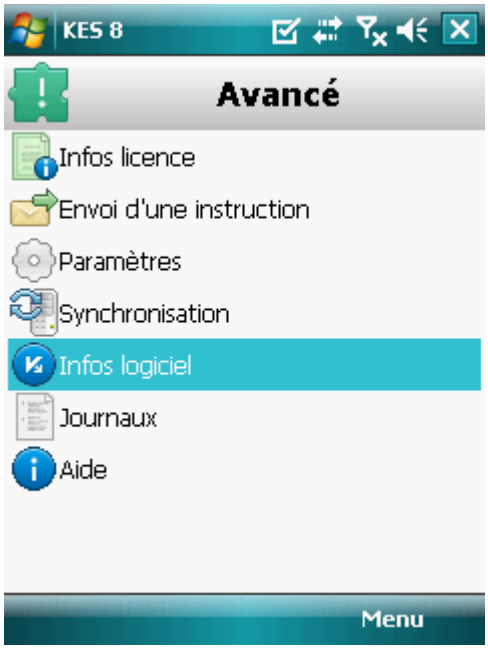

Figure 7: informations sur l'application

INTERFACE DE L'APPLICATION

Cette section présente des informations sur les principaux composants de l'interface de Kaspersky Endpoint Security 8 for Smartphone.

DANS CETTE SECTION

FENETRE D'ETAT DE LA PROTECTION

L'état des composants principaux de l'application s'affiche dans la fenêtre de l'état de la protection.

Il existe trois états possibles pour chaque composant. Chacun d'entre eux est associé à une couleur, comme les feux de circulation. Le vert signifie que la protection de l'appareil est assurée au niveau requis. Le jaune et le rouge signalent des menaces de sécurité de nature différente. Les menaces groupent non seulement des bases antivirus dépassées, mais aussi des composants de la protection désactivés, des paramètres de base minimum de l'application etc.

La fenêtre de l'état de la protection est accessible directement après le lancement de l'application et reprend les informations suivantes :

- **Protection** : état de la protection en temps réel (cf. la rubrique «Protection en temps réel» à la page 30).

  L'icône verte de l'état indique que la protection est activée et assurée au niveau requis. Les bases antivirus de l'application sont à jour.

  L'icône jaune signale que la mise à jour des bases antivirus n'a plus eu lieu depuis quelques jours.

  L'icône rouge signale des problèmes qui pourraient entraîner la perte d'informations ou l'infection de l'appareil : par exemple, si la protection de l'application est désactivée ou si l'application n'a pas été actualisée depuis plus de deux semaines.

- **Pare-feu** : le niveau de protection de l'appareil contre l'activité de réseau indésirable (cf. la rubrique «Filtrage de l'activité de réseau. Pare-feu» à la page 73).

  L'icône verte de l'état signifie que le composant est activé. Le mode Pare-feu est sélectionné.

  L'icône rouge signale que le composant Pare-feu est désactivé.

- **Antivol** : état de la protection des données en cas de vol ou de perte de l'appareil (cf. la rubrique «Protection des données en cas de perte ou de vol de l'appareil» à la page 54).

  L'icône verte signifie que les fonctions de l'Antivol dont le nom apparaît sous l'état du composant sont activées.

  L'icône rouge indique que toutes les fonctions de l'Antivol sont désactivées.

- **Contacts personnels** : état de la dissimulation des informations confidentielles (cf. la rubrique «Dissimulation des informations confidentielles» à la page 64).

  L'icône verte de l'état signifie que la dissimulation des informations confidentielles est activée. Les informations confidentielles sont masquées.

  L'icône jaune prévient l'utilisateur que la dissimulation des informations confidentielles est désactivée. Les informations confidentielles sont affichées et peuvent être consultées.

- **Licence** : durée de validité de la licence (cf. la rubrique «Administration des licences» à la page 19).

  L'icône verte d'état indique que la licence est encore valide pendant plus de 14 jours.

  L'icône jaune indique que la licence est valide pour moins de 14 jours.

  L'icône rouge indique que votre licence a expiré ou que la licence n'a pas été installée.

Figure 8: Fenêtre de l'état de la protection

Vous pouvez aussi passer à la fenêtre de l'état de la protection en choisissant l'option **Menu** → **Etat de la protection**.

MENU DE L'APPLICATION

Les composants de l'application sont regroupés logiquement et accessibles dans le menu de l'application. Chaque option du menu permet d'accéder aux paramètres du composant sélectionné ainsi qu'aux tâches de la protection (cf. ill. ci-après).

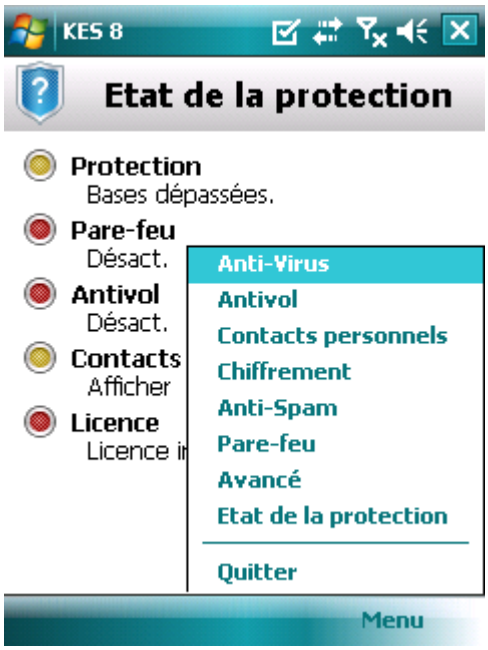

Figure 9: menu de l'application

Le menu Kaspersky Endpoint Security 8 for Smartphone reprend les points suivants :

- **Anti-Virus :** protection du système de fichiers contre les virus, analyse à la demande et actualisation des bases antivirus de l'application.
- **Antivol** : protège des données stockées sur l'appareil en cas de perte ou de vol.
- **Contacts personnels** : masque les informations confidentielles sur l'appareil.
- **Chiffrement** : chiffre les données stockées sur l'appareil.
- **Anti-Spam** : filtrage des SMS et des appels entrants non sollicités.
- **Pare-feu** : contrôle l'activité de réseau.
- **Avancé** : paramètres généraux de l'application, lancement de la synchronisation de l'appareil avec le système d'administration distante, information sur l'application et sur la licence.
- **Etat de protection** : informations sur les composants principaux de l'application.
- **Quitter** : quitte la configuration de l'application.

Pour ouvrir le menu de l'application,

sélectionnez **Menu**.

Pour naviguer dans le menu de l'application, utilisez le joystick de l'appareil ou le stylet.

Pour revenir à la fenêtre d'état des composants logiciels,

sélectionnez **Menu** → **Etat de la protection**.

Pour quitter le programme,

sélectionnez **Menu** → **Quitter**.

PROTECTION DU SYSTEME DE FICHIERS

La rubrique présente des informations sur le composant Protection qui permet d'éviter l'infection du système de fichiers de l'appareil. La section explique aussi comment activer / suspendre la protection et la configurer.

DANS CETTE SECTION

PRESENTATION DE LA PROTECTION

La protection est lancée en même temps que le système d'exploitation et se trouve en permanence dans la mémoire vive de l'appareil. La Protection surveille en arrière-plan les modifications introduites dans le système de fichiers et vérifie si celui-ci contient des objets malveillants. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. La protection analyse chaque fichier au moment où l'utilisateur essaie de l'accéder.
2. La protection analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparants aux bases antivirus utilisées par le logiciel. Les bases antivirus contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.
3. Après l'analyse, la Protection agit en fonction de ses résultats :
   - quand du code malveillant est découvert dans le fichier, la protection le bloque et agit conformément aux paramètres définis ;
   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Les informations sur les résultats du fonctionnement de la protection sont consignées dans le journal de l'application (cf. la rubrique «Journaux de l'application» à la page 86).

L'ACTIVATION / LA DESACTIVATION DE LA PROTECTION

Lorsque la protection est activée, toutes les actions exécutées dans le système sont placées sous un contrôle permanent.

La protection contre les virus et autres programmes malveillants usent les ressources de l'application. Pour diminuer la charge sur l'appareil lors de l'exécution de plusieurs tâches, vous pouvez suspendre temporairement la protection.

Les spécialistes de Kaspersky Lab recommandent de ne pas désactiver la protection car cela pourrait entraîner l'infection de l'appareil et la perte de données.

La désactivation de la protection n'affecte pas les tâches d'analyse antivirus et de mise à jour des bases antivirus de l'application.

L'état actuel de la protection est repris sur l'écran **Anti-Virus** à côté de l'option de menu **Protection**.

Vous pouvez activer/désactiver la protection d'une des méthodes suivantes :

- depuis le menu de configuration du composant ;
- depuis le menu **Anti-Virus**.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

- *Pour désactiver la protection, procédez de la manière suivante :*

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Protection**.

   L'écran **Protection** s'ouvre.

3. Cochez la case **Activer la protection** (cf. ill. ci-après).

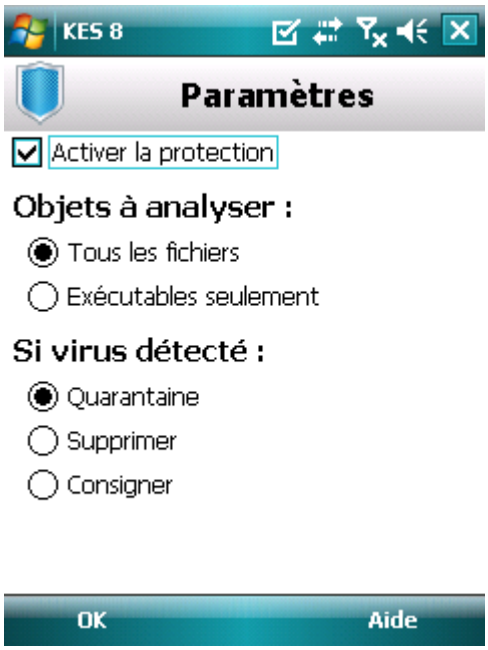

Figure 10 : activation de la protection

4. Appuyez sur **OK** pour enregistrer les modifications.

- *Pour désactiver la protection, procédez de la manière suivante :*

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Protection**.

   L'écran **Protection** s'ouvre.

3. Désélectionnez la case **Activer la protection**.

4. Appuyez sur **OK** pour enregistrer les modifications.

- *Pour activer/désactiver la protection, procédez comme suit :*

1. Sélectionnez **Menu** → **Anti-Virus**.

2. L'écran **Anti-Virus** apparaît.

3. Appuyez sur **Activer** / **Désactiver**. Le texte de l'option du menu prendra la valeur opposée en fonction de l'état actuel de la protection.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS MALVEILLANTS

Vous pouvez sélectionner l'action que Kaspersky Endpoint Security 8 for Smartphone exécute sur l'objet malveillant découvert.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour modifier la valeur des paramètres de la protection, assurez-vous qu'elle est activée.

Pour définir l'action que l'application exécutera sur l'objet malveillant découvert, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Protection**.

   L'écran **Protection** s'ouvre.

3. Définissez l'action que l'application exécutera sur l'objet malveillant découvert. Pour ce faire, attribuez une valeur au paramètre Si un virus est découvert (cf. ill. ci-après) :

   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Consigner :** ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application et bloque les tentatives d'accès à l'objet (par exemple, copie ou ouverture).

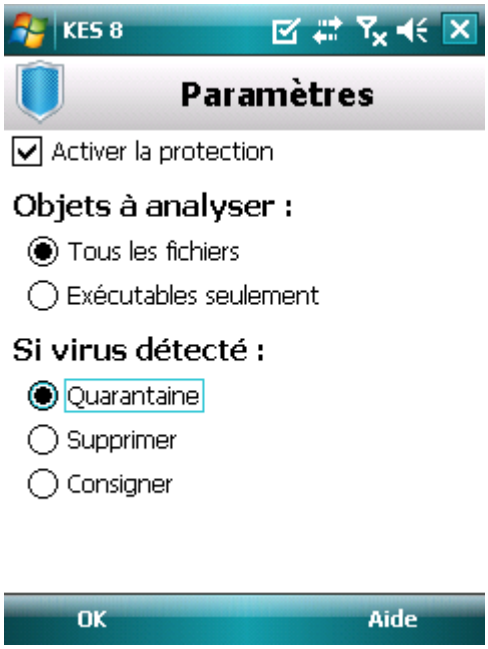

Figure 11: Sélection de l'action lors détection d'une menace

4. Appuyez sur **OK** pour enregistrer les modifications.

ANALYSE DE L'APPAREIL

Cette section présente les informations sur l'analyse de l'appareil à la demande, qui permet d'identifier et de neutraliser les menaces sur votre appareil. De plus, la section décrit comment lancer l'analyse de l'appareil, comment configurer l'analyse programmée du système de fichiers, comment sélectionner les fichiers à analyser et définir l'action de l'application en cas de détection d'une menace.

DANS CETTE SECTION

À PROPOS DE L'ANALYSE A LA DEMANDE

L'analyse à la demande permet d'identifier et de neutraliser les objets malveillants. Kaspersky Endpoint Security 8 for Smartphone permet de réaliser une analyse complète ou partielle de l'appareil. En cas d'analyse partielle l'application peut analyser uniquement le contenu de la mémoire intégrée de l'appareil ou un dossier spécifique (y compris les dossiers stockés sur la carte mémoire).

L'analyse de l'appareil s'opère selon l'algorithme suivant :

1. Kaspersky Endpoint Security 8 for Smartphone analyse les fichiers, définis dans les paramètres de vérification (cf. la rubrique «Sélection du type d'objet à analyser» à la page 35).
2. Pendant la vérification, l'application analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparants aux bases antivirus utilisées par le logiciel. Les bases antivirus contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.
3. Après l'analyse, Kaspersky Endpoint Security 8 for Smartphone agit en fonction de ses résultats :
   - · Quand un code malveillant est découvert dans un fichier, Kaspersky Endpoint Security 8 for Smartphone bloque le fichier et exécute l'action sélectionnée conformément aux paramètres définis (cf. la rubrique «Sélection des actions à appliquer sur des objets» à la page 37) ;
   - Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

L'analyse est lancée manuellement ou automatiquement selon un horaire prédéfini (cf. rubrique «Exécution de l'analyse programmée» à la page 35).

Les informations sur les résultats de l'analyse à la demande sont consignées dans le journal de l'application (cf. la rubrique «Journaux de l'application» à la page 86).

EXECUTION MANUELLE D'UNE ANALYSE

Vous pouvez lancer l'analyse complète ou partielle à la demande en mode manuel, par exemple, lorsque le processeur de l'application n'exécute pas d'autres tâches.

Pour lancer une analyse, procédez de la manière suivante :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyse**.

   L'écran **Analyse** s'ouvre.

3. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :

   - **Analyse complète** : analyse tout le système de fichiers de l'application. L'application analyse par défaut les fichiers stockés dans la mémoire de l'appareil et sur les cartes mémoire.
   - **Analyse de la mémoire** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.
   - **Analyser dossier** : analyse un dossier sélectionné du système de fichiers de l'appareil ou sur une carte mémoire. Si cette option est sélectionnée, l'application affiche l'écran de sélection du dossier à analyser avec l'arborescence du système de fichiers de l'appareil. Utilisez le stylet ou les boutons du joystick pour vous déplacer dans le système de fichiers. Pour lancer l'analyse du dossier, sélectionnez le dossier requis, puis appuyez sur **Analyser**.

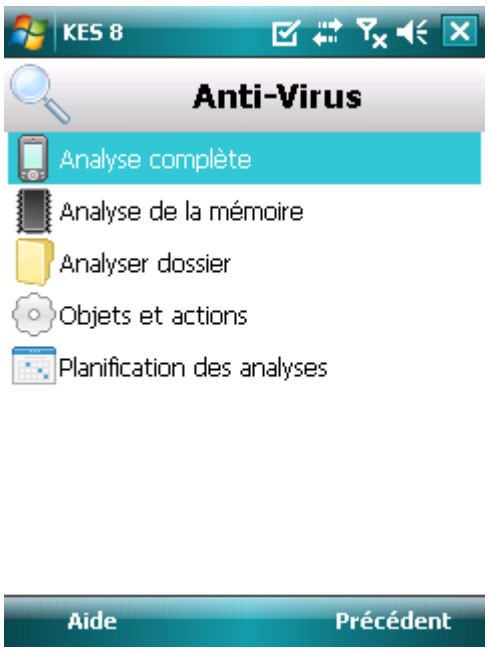

Figure 12: sélection de la zone d'analyse

   Après le démarrage de l'analyse, une fenêtre affiche l'état actuel de la tâche : nombre d'objets analysés, chemin de l'objet en cours d'analyse.

   Si Kaspersky Endpoint Security 8 for Smartphone détecte un objet infecté, l'application exécute l'action définie dans les paramètres de vérification (cf. la rubrique «Sélection de l'action sur les objets détectés» à la page 37).

   A la fin de l'analyse, l'application affiche sur l'écran les informations suivantes :

   - Le nombre de fichiers analysés ;
   - Le nombre des objets malveillants découverts, placés en quarantaine et supprimés ;
   - Le nombre des fichiers ignorés (par exemple, lorsque le fichier est bloqué par le système d'exploitation ou lorsque le fichier n'est pas un fichier exécutable alors que l'analyse porte uniquement sur les fichiers exécutables) ;
   - L'heure de l'analyse.

4. A la fin, cliquez sur **OK**.

EXECUTION DE L'ANALYSE PROGRAMMEE

Kaspersky Endpoint Security 8 for Smartphone permet de configurer le lancement automatique de l'analyse programmée du système de fichiers. L'analyse est exécutée en arrière-plan. Quand un objet infecté est détecté, l'application exécute l'action sélectionnée dans la configuration de l'analyse (cf. section «Sélection des actions à appliquer sur les objets identifiés» à la page 37).

L'analyse programmée ne sera exécutée que si l'appareil est allumé pendant la période d'analyse.

Pour configurer le lancement automatique de l'analyse programmée et programmer le lancement de l'analyse, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyse**.

   L'écran **Analyse** s'ouvre.

3. Sélectionnez l'option **Planification des analyses**.

   L'écran **Programmation** s'ouvre.

4. Cochez la case **Analyse programmée** (cf. ill. ci-après).

5. Sélectionnez l'intervalle de lancement de l'analyse. Pour ce faire, sélectionnez une des valeurs proposées pour le paramètre **Fréquence** :

   - **Chaque jour** : l'analyse s'exécutera tous les jours. Indiquez l'heure de lancement dans le champ **Heure**.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Indiquez l'heure et le jour de lancement de l'analyse. Pour ce faire, saisissez les valeurs des paramètres **Heure** et **Jour de la semaine**.

Figure 13: programmation du lancement de l'analyse complète

6. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DU TYPE D'OBJET A ANALYSER

Vous pouvez définir les types de fichiers que l'application va analyser pendant l'Analyse à la demande.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour sélectionner le type de fichiers à analyser, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyse**.

   L'écran **Analyse** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

   L'écran **Objets et actions** s'ouvre.

4. Sélectionnez le type de fichiers analysés dans le groupe **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Exécutables seulement** : analyse uniquement les fichiers exécutables des applications au format EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

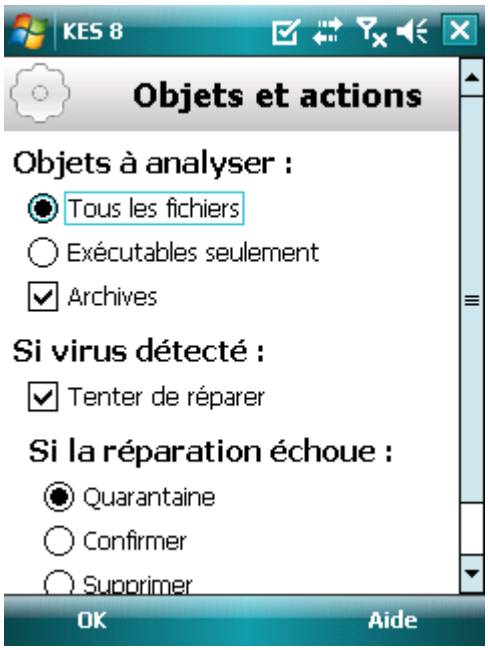

Figure 14: sélection du type de fichiers à analyser

5. Appuyez sur **OK** pour enregistrer les modifications.

CONFIGURATION DE L'ANALYSE DE FICHIERS COMPRESSES

Souvent, les virus se dissimulent dans des archives. L'application permet d'analyser les archives des formats suivants : ZIP, JAR, JAD et CAB. Pendant l'analyse, les archives sont décompressées, ce qui peut réduire sensiblement la vitesse de l'Analyse à la demande.

Vous pouvez activer / désactiver l'analyse du contenu des archives pendant l'Analyse à la demande pour détecter des codes malveillants éventuels.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour activer l'analyse du contenu des archives, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyse**.

   L'écran **Analyse** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

   L'écran **Objets et actions** s'ouvre.

4. Dans le groupe **Objets à analyser**, cochez la case **Archives**.

5. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Quand un code malveillant est découvert dans un fichier, Kaspersky Endpoint Security 8 for Smartphone bloque l'action et exécute l'action sélectionnée conformément aux paramètres définis.

Vous pouvez modifier l'action que l'application exécutera sur l'objet malveillant découvert.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour définir l'action que l'application exécutera sur l'objet malveillant découvert, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyse**.

   L'écran **Analyse** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

   L'écran **Objets et actions** s'ouvre.

4. Pour que le programme tente de réparer les objets infectés, cochez la case **Tenter de réparer** pour le paramètre **Action Anti-Virus** (cf. ill. ci-après).

5. Définissez l'action à exécuter sur les objets malveillants découverts. Pour ce faire, attribuez une valeur au paramètre **Exécuter l'action** :

   Si la case **Tenter de réparer** avait été cochée, le paramètre s'appelle **Si la réparation échoue**. Ce paramètre détermine l'action de l'application en cas d'échec de la réparation.

   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Interroger** : demande une confirmation de l'action à l'utilisateur en cas de découverte d'objets malveillants.
   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application.

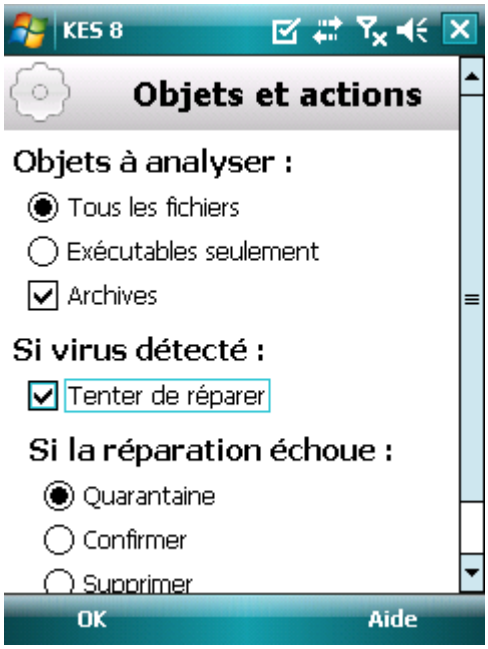

Figure 15: Sélection de l'action lors détection d'une menace

6. Appuyez sur **OK** pour enregistrer les modifications.

QUARANTAINE DES OBJETS MALVEILLANTS

La rubrique présente les informations relatives à la *quarantaine*, un dossier spécial où sont placés les objets potentiellement dangereux. De plus, elle décrit comment consulter, restaurer ou supprimer les objets malveillants stockés dans le dossier.

DANS CETTE SECTION

À PROPOS DE LA QUARANTAINE

L'application place les objets malveillants détectés en *quarantaine* dans un dossier spécial isolé pendant l'analyse de l'appareil ou pendant le fonctionnement de la protection. Les objets malveillants placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil.

Vous pouvez consulter les fichiers placés en quarantaine, les supprimer ou les restaurer.

AFFICHAGE DES OBJETS EN QUARANTAINE

Vous pouvez consulter la liste des objets malveillants, que l'application a mis en quarantaine. Le nom complet de l'objet dans la liste et la date à laquelle il a été découvert sont repris.

Vous pouvez également consulter des informations complémentaires sur l'objet malveillant sélectionné : chemin d'accès à l'objet sur l'appareil avant sa mise en quarantaine et nom de la menace.

- *Pour consulter la liste des objets en quarantaine, procédez comme suit :*

  1. Sélectionnez **Menu** → **Anti-Virus**.

     L'écran **Anti-Virus** apparaît.

  2. Sélectionnez l'option **Quarantaine**.

     L'écran **Quarantaine** s'ouvre et présente la liste des objets placés en quarantaine (cf. ill. ci-après).

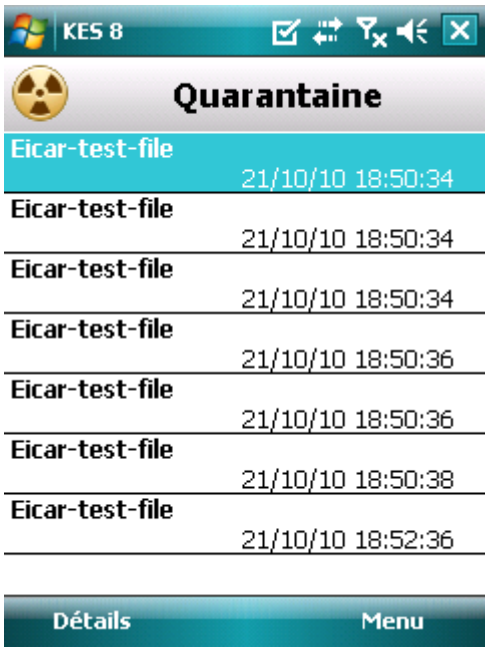

Figure 16 : liste des fichiers placés en quarantaine

- *Pour consulter les informations relatives à l'objet infecté,*

  cliquez **Détails**.

L'écran **Détails** présente les informations suivantes sur l'objet : chemin d'accès au fichier sur l'appareil avant sa détection et nom du virus.

L'écran **Détails** s'ouvre.

RESTAURATION D'OBJETS DE LA QUARANTAINE

Si vous êtes convaincu que l'objet découvert ne constitue pas une menace pour l'appareil, vous pouvez le restaurer depuis la quarantaine. L'objet restauré sera remis dans on répertoire d'origine.

Pour restaurer un objet depuis la quarantaine, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.

3. Sélectionnez l'objet à restaurer, puis choisissez l'option **Menu** → **Restaurer**.

L'objet sélectionné dans la quarantaine est restauré dans son dossier d'origine.

SUPPRESSION D'OBJETS DE LA QUARANTAINE

Il est possible de supprimer un objet placé en quarantaine ou l'ensemble des objets placés en quarantaine.

Pour supprimer un objet de la quarantaine, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.

3. Sélectionnez l'objet à supprimer, puis choisissez l'option **Menu** → **Supprimer**.

L'objet sélectionné est supprimé de la quarantaine.

Pour supprimer tous les objets de la quarantaine, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.

3. Appuyez sur **Menu** → **Supprimer tout**.

Tous les objets en quarantaine seront éliminés.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

Cette section présente les informations sur l'Anti-Spam qui interdit la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche que vous avez créées. De plus, la section décrit comment sélectionner le mode de filtrage Anti-Spam des appels et des SMS entrants, comment configurer les paramètres avancés de filtrage pour les appels et les SMS entrants et comment créer la liste noire et la liste blanche.

DANS CETTE SECTION

A PROPOS DE L'ANTI-SPAM

L'Anti-Spam empêche la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche que vous avez créées.

Les listes contiennent les enregistrements. L'enregistrement dans chaque liste contient les informations suivantes :

- Numéro de téléphone que l'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche.
- Type d'événement que l'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche. Types d'informations représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à l'Anti-Spam d'identifier si les SMS sont sollicités ou non. S'il s'agit de la liste noire, l'Anti-Spam va refuser les SMS avec cette expression clé et accepter les autres SMS sans cette expression clé. S'il s'agit des numéros de la liste blanche, l'Anti-Spam va accepter les SMS avec cette expression clé et refuser les SMS sans cette expression clé.

L'Anti-Spam filtre les appels et les SMS entrants selon le mode sélectionné (cf. la rubrique «Présentation des modes de l'Anti-Spam» à la page 42). L'Anti-Spam analyse, sur la base du régime, chaque SMS ou appel entrant et détermine si ce SMS ou cet appel est sollicité ou non. L'analyse se termine dès que l'Anti-Spam a attribué l'état de sollicité ou non au SMS ou à l'appel.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section « Journaux du logiciel» à la page 86).

PRESENTATION DES MODES DE L'ANTI-SPAM

Le mode détermine les règles utilisées par l'Anti-Spam pour filtrer les appels et les SMS entrants.

Les modes de fonctionnement de l'Anti-Spam disponibles :

- **Désactivé** : accepte tous les appels et les SMS entrants.
- **Autoriser la Liste blanche** : accepte uniquement les appels et les SMS en provenance des numéros de la liste blanche.
- **Bloquer la Liste noire** : accepte tous les appels et les SMS, sauf ceux qui proviennent des numéros de la liste noire.
- **Les deux listes** : accepte les appels et les SMS en provenance des numéros de la liste blanche et interdit ceux qui proviennent des numéros de la liste noire. Après la conversation ou la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, l'Anti-Spam vous invitera à ajouter ce numéro sur une des listes.

Vous pouvez modifier le mode de l'Anti-Spam (cf. la rubrique « Modification du mode de l'Anti-Spam» à la page 43). Le mode actuel de l'Anti-Spam s'affiche à l'écran **Anti-Spam** à côté de l'option **Mode**.

MODIFICATION DU MODE DE L'ANTI-SPAM

Pour sélectionner le mode de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Sélectionnez une valeur pour le paramètre **Mode Anti-Spam** (cf. ill. ci-dessous).

Figure 17: modification du mode de l'Anti-Spam

4. Appuyez sur **OK** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Les enregistrements de la liste noire contiennent les numéros de téléphone interdits dont les appels et les SMS sont refusés par l'Anti-Spam. Chacun de ces enregistrements contient les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par l'Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Anti-Spam bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à l'Anti-Spam d'identifier des SMS non sollicités (spam). L'Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

L'Anti-Spam bloquera uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste noire. L'Anti-Spam acceptera les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste noire.

Il est impossible d'ajouter le même numéro de téléphone avec les mêmes critères de filtrage sur la liste noire et sur la liste blanche.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section « Journaux du logiciel» à la page 86).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE NOIRE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Endpoint Security 8 for Smartphone vous prévient : le message de circonstance s'affiche.

Pour ajouter une entrée dans la liste noire de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Sélectionnez **Menu** → **Ajouter**.

   L'écran **Nouvel enregistrement** s'ouvre.

4. Attribuez des valeurs aux paramètres suivants (cf. ill. ci-après) :

   - **Bloquer tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste noire :
     - **Appels et SMS** : bloque les appels et les SMS entrants.
     - **Appels seulement :** bloque uniquement les appels entrants.
     - **SMS seulement** : bloque uniquement les SMS entrants.
   - **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par l'Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe “+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques “*» et “?» (où “*» représente n'importe quel nombre de caractères et “?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la Liste noire. L'Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenants le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). L'Anti-Spam refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS.

   Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Contenant le texte** de cette entrée, vide.

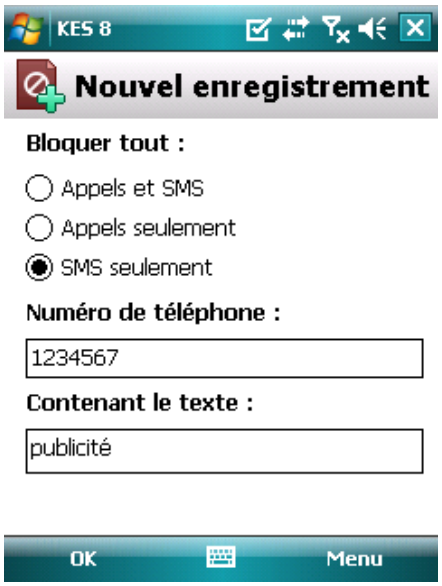

Figure 18 : paramètres d'une entrée de la liste noire

5. Appuyez sur **OK** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Dans les enregistrements de la liste noire des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier un enregistrement de la liste noire de l'Anti-Spam, exécutez les opérations suivantes :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

   L'écran **Modifier entrée** s'ouvre.

4. Modifiez les paramètres requis.

   - **Bloquer tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste noire :
     - **Appels et SMS** : bloque les appels et les SMS entrants.
     - **Appels seulement :** bloque uniquement les appels entrants.
     - **SMS seulement** : bloque uniquement les SMS entrants.
   - **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par l'Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe “+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques “*» et “?» (où “*» représente n'importe quel nombre de caractères et “?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la Liste noire. L'Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenants le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). L'Anti-Spam refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS.

   Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Contenant le texte** de cette entrée, vide.

5. Appuyez sur **OK** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer ce numéro de la liste noire. De plus, vous pouvez purger la liste noire de l’Anti-Spam en supprimant tous les enregistrements qu'elle contient.

Pour supprimer un enregistrement de la liste noire de l’Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
4. Confirmez la suppression de l'entrée. Pour ce faire, cliquez sur **Oui**.

Pour purger la liste noire de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Sélectionnez l'option **Menu** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Les enregistrements de la Liste blanche contiennent les numéros de téléphone autorisés dont les appels et les SMS sont acceptés par l'Anti-Spam. Chacun de ces enregistrements contient les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par l'Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Anti-Spam accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à l'Anti-Spam d'identifier des SMS sollicités (qui ne sont pas du spam). L'Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

L'Anti-Spam accepte uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste blanche. L'Anti-Spam refuse les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste blanche.

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Endpoint Security 8 for Smartphone vous prévient : le message de circonstance s'affiche.

Pour ajouter un enregistrement à la liste blanche de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Sélectionnez **Menu** → **Ajouter**.

   L'écran **Nouvel enregistrement** s'ouvre.

4. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste blanche :
     - **Appels et SMS** : autorise les appels et les SMS entrants.
     - **Appels seulement :** autorise uniquement les appels entrants.
     - **SMS seulement** : autorise les messages SMS entrants uniquement.
   - **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par l'Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe “+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques “*» et “?» (où “*» représente n'importe quel nombre de caractères et “?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. L'Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, l'Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro.

   Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cette entrée, vide.

Figure 19 : paramètres d'une entrée de la liste blanche

5. Appuyez sur **OK** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier un enregistrement de la liste blanche de l'Anti-Spam, exécutez les opérations suivantes :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez **Menu** → **Modifier**.

   L'écran **Modifier** s'ouvre.

4. Modifiez les paramètres requis.

   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste blanche :
     - **Appels et SMS** : autorise les appels et les SMS entrants.
     - **Appels seulement :** autorise uniquement les appels entrants.
     - **SMS seulement** : autorise les messages SMS entrants uniquement.
   - **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par l'Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe “+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques “*» et “?» (où “*» représente n'importe quel nombre de caractères et “?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. L'Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, l'Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro.

   Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cette entrée, vide.

5. Appuyez sur **OK** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer une seule entrée de la liste blanche ou purger la liste.

Pour supprimer un enregistrement de la liste blanche de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
4. Confirmez la suppression de l'entrée. Pour ce faire, cliquez sur **Oui**.

Pour purger la liste blanche de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Sélectionnez l'option **Menu** → **Supprimer tout**.

La liste est désormais vide.

REACTION AUX SMS ET AUX APPELS EN PROVENANCE DES NUMEROS QUI NE FIGURENT PAS DANS LES CONTACTS

Si le mode choisi pour l'Anti-Spam est **Les deux listes** ou **Liste blanche** (cf. la rubrique "**Présentation des modes de l'Anti-Spam**» à la page 42), vous pouvez enrichir la liste blanche. Dans ce cas, l'Anti-Spam traite les appels et les SMS en provenance des numéros des Contacts comme s'il s'agit des numéros de la liste blanche.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour enrichir la liste blanche en y ajoutant les numéros des Contacts, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Mode**.
3. L'écran **Mode** s'ouvre.
4. Choisissez la valeur de paramètre **Autoriser contacts** (cf. ill. ci-après) :
   - Pour que l'Anti-Spam considère un numéro des contacts comme un ajout à la liste blanche et qu'il n'accepte pas les SMS et les appels en provenance de numéros qui ne figurent pas dans les Contacts, cochez la case **Autoriser contacts** ;
   - Pour que l'Anti-Spam filtre les SMS et les appels uniquement sur la base du régime défini de l'Anti-Spam, décochez la case **Autoriser contacts**.

Figure 20: réaction de l'Anti-Spam face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

5. Appuyez sur **OK** pour enregistrer les modifications.

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode **Les deux listes** ou **Bloquer la Liste noire** (cf. la rubrique "**Présentation des modes de l'Anti-Spam**» à la page 43) de l'Anti-Spam a été sélectionné, vous pouvez enrichir la liste noire en incluant tous les numéros sans chiffres (composés de lettres). Si cette case est cochée, l'Anti-Spam traite les appels et les SMS en provenance des numéros sans chiffres comme s'il s'agit des numéros de la liste noire.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour enrichir la liste noire en y ajoutant tous les numéros sans chiffres, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Choisissez une valeur pour le paramètre **Exclure appels non numériques** (cf. ill. ci-après) :

   - afin que l'Anti-Spam bloque les messages en provenance de numéros sans chiffres, cochez la case **Exclure appels non numériques** ;
   - afin que l'Anti-Spam filtre les SMS en provenance de numéros sans chiffres sur la base du mode sélectionné pour l'Anti-Spam, décochez la case **Exclure appels non numériques**.

Figure 21: Sélection des actions exécutées par l'Anti-Spam en cas de réception de SMS depuis un numéro sans chiffres

4. Appuyez sur **OK** pour enregistrer les modifications.

DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

Si le mode choisi est **Les deux listes** (cf. la rubrique "**Présentation des modes de l'Anti-Spam**» à la page 42), l'Anti-Spam analyse les SMS entrants sur la base des listes blanche et noire.

Après la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, l'Anti-Spam suggère d'ajouter ce numéro sur une des listes (cf. ill. ci-après).

Figure 22: notification de l'Anti-Spam sur le SMS reçu

Vous pouvez choisir l'une des actions suivantes à appliquer sur le SMS :

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste noire, sélectionnez **Menu** → **Ajouter à la liste noire**.
- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste blanche, sélectionnez **Menu** → **Ajouter à la liste blanche**.
- Pour accepter le SMS sans consigner le numéro de téléphone de l'appelant dans aucune des listes, appuyez sur **Ignorer**.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal de l'application (cf. section Journaux de l'application à la page 86).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Si le mode choisi est **Les deux listes** (cf. la rubrique "**Présentation des modes de l'Anti-Spam**» à la page 42), l'Anti-Spam analyse les appels entrants sur la base des listes blanche et noire. Après la réception d'un appel en provenance du numéro qui ne figure sur aucune des listes, l'Anti-Spam suggère d'ajouter ce numéro sur une des listes (cf. ill. ci-après).

Figure 23: notification de l'Anti-Spam sur l'appel reçu

Vous pouvez choisir une des actions suivantes pour le numéro de l'appelant (cf. ill. ci-après) :

- Pour ajouter le numéro de téléphone de l'appelant à la liste noire, sélectionnez **Menu** → **Ajouter à la liste noire**.
- Pour ajouter le numéro de téléphone de l'appelant à la liste blanche, sélectionnez **Menu** → **Ajouter à la liste blanche**.
- Choisissez **Ignorer** si vous ne souhaitez pas consigner le numéro de l'appelant dans aucune des listes.

Les informations relatives aux appels bloqués sont consignées dans le journal de l'application.

PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL

La section présente le composant Antivol, qui protège les données stockées sur l'appareil mobile contre l'accès non autorisé en cas de perte ou de vol, toute en facilitant sa recherche.

Elle explique également comment activer/désactiver les fonctions de l'Antivol, configurer les paramètres de fonctionnement et comment lancer à distance la fonction Antivol depuis un autre appareil mobile.

DANS CETTE SECTION

À PROPOS DU COMPOSANT ANTIVOL

Antivol protège les données sur votre appareil mobile contre l'accès non autorisé.

Antivol dispose des fonctions suivantes :

- **Verrouillage** permet de verrouiller l'appareil à distance et de définir le texte qui apparaîtra à l'écran de l'appareil bloqué.
- **Suppression** permet de supprimer à distance les données personnelles de l'utilisateur (entrées dans les Contacts, SMS, galerie, calendrier, journaux, paramètres de connexion à Internet), ainsi que les données de la carte mémoire et les dossiers de la liste à supprimer.
- **SIM-Surveillance** permet de garder le numéro de téléphone en cas de remplacement de la carte SIM et de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte. Le message avec le nouveau numéro de téléphone est envoyé vers le numéro de téléphone et/ou l'adresse de la messagerie électronique que vous avez spécifié.
- **Géolocalisation** : permet de déterminer les coordonnées de l'appareil. Le message avec les coordonnées géographiques de l'appareil est envoyé au numéro de téléphone qui a émis le SMS spécial, ainsi que à l'adresse de la messagerie électronique.

Kaspersky Endpoint Security 8 for Smartphone permet de lancer à distance la fonction Antivol via l'envoi d'une instruction SMS (cf. la rubrique “Lancement à distance de la fonction Antivol» à la page 63) depuis un autre appareil mobile.

Pour exécuter les fonctions Antivol à distance, il faudra utiliser le code secret de l'application qui a été défini à la première exécution de Kaspersky Endpoint Security 8 for Smartphone.

L'état actuel de chaque fonction apparaît dans l'écran **Antivol** à côté du nom de l'application.

Les informations relatives au fonctionnement du composant sont consignées dans le journal de l'application (cf. section « Journaux de l'application » à la page 86).

VERROUILLAGE DE L'APPAREIL

Après la réception d'une instruction SMS spéciale, la fonction Verrouillage permet de verrouiller à distance l'accès à l'appareil et aux données qu'il renferme. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Cette fonction ne verrouille pas l'appareil mais active uniquement la possibilité de le verrouiller à distance.

Pour activer la fonction de verrouillage, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Sélectionnez l'option **Verrouillage**.

   L'écran **Verrouillage** s'ouvre.

3. Cochez la case **Activer le Verrouillage**.

4. Dans le champ **Texte en cas de verrouillage**, modifiez le message qui apparaîtra sur l'écran de l'appareil verrouillé (cf. ill. ci-après). Un texte standard est utilisé par défaut. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

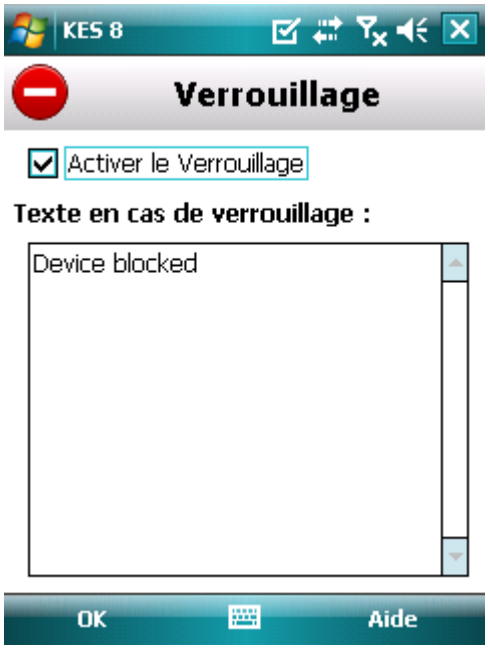

Figure 24: paramètres de la fonction Verrouillage

5. Appuyez sur **OK** pour enregistrer les modifications.

Pour verrouiller un autre appareil, si la fonction Verrouillage est activée, vous disposez des méthodes suivantes :

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction **Envoi d'une instruction**. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour verrouiller l'appareil à distance, il est conseillé d'utiliser une méthode sûre en exécutant la fonction Envoi d'une instruction. Dans ce cas, le code secret est envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Sélectionnez l'instruction SMS** la valeur **Verrouillage** (cf. ill. ci-après).
4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
5. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

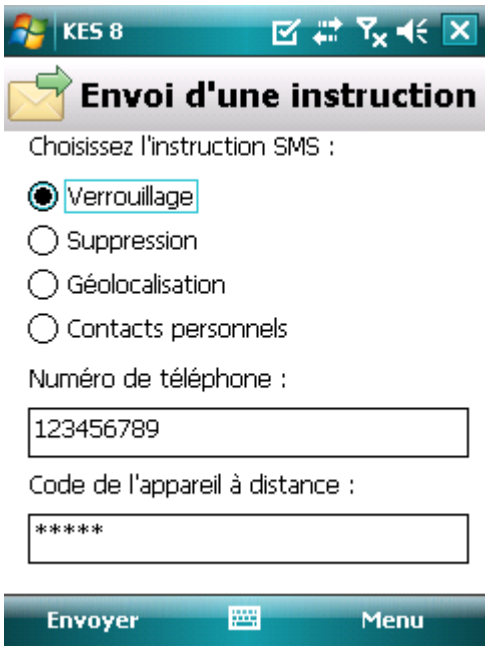

Figure 25: Activation de la fonction de Verrouillage à distance

6. Appuyez sur **Envoyer**.

Pour composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,

envoyez à un autre appareil un SMS contenant le texte `block:<code>` (où `<code>` est le code secret défini sur un autre appareil à verrouiller). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

SUPPRESSION DE DONNEES PERSONNELLES

Après la réception de l'instruction SMS spéciale, la fonction Suppression permet de supprimer les informations suivantes sur l'appareil :

- données personnelles de l'utilisateur (entrées des Contacts et sur la carte SIM, SMS, galerie, calendrier, paramètres de connexion à Internet) ;
- données sur la carte mémoire ;
- Les fichiers du dossier **Mes documents** et d'autres dossiers de la liste **Dossiers à supprimer**.

Cette fonction ne supprime pas les données enregistrées sur l'appareil mais active la possibilité de le faire après la réception de l'instruction SMS.

Pour activer la fonction de suppression des données, procédez comme suit :

1. Choisissez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

   L'écran **Suppression de données** s'ouvre.

3. Sélectionnez l'option **Mode**.

   L'écran **Suppression de données** s'ouvre.

4. Cochez la case **Activer la suppression de données**.

5. Sélectionnez les données à supprimer après la réception de l'instruction SMS spéciale. Pour ce faire, dans le groupe **Supprimer**, cochez les cases en regard des paramètres requis (cf. ill. ci-après) :

   - Pour supprimer les données personnelles, cochez la case **Données personnelles** ;
   - Pour supprimer les fichiers du dossier **Mes documents** et de la liste **Dossiers à supprimer**, cochez la case **Dossiers à supprimer**.

Figure 26: Sélection des informations à supprimer.

6. Appuyez sur **OK** pour enregistrer les modifications.
7. Passez à la constitution de la liste **Dossiers à supprimer** (cf. rubrique “**Composition de la liste des objets à supprimer**» à la page 59).

La suppression des données personnelles de l'appareil peut être réalisée d'une des manières suivantes :

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour supprimer à distance les informations de l'appareil, il est conseillé d'utiliser une méthode sûre en exécutant la fonction Envoi d'une instruction. Dans ce cas, le code secret est envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Choisissez l'instruction SMS** la valeur **Suppression** (cf. ill. ci-après).
4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
5. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

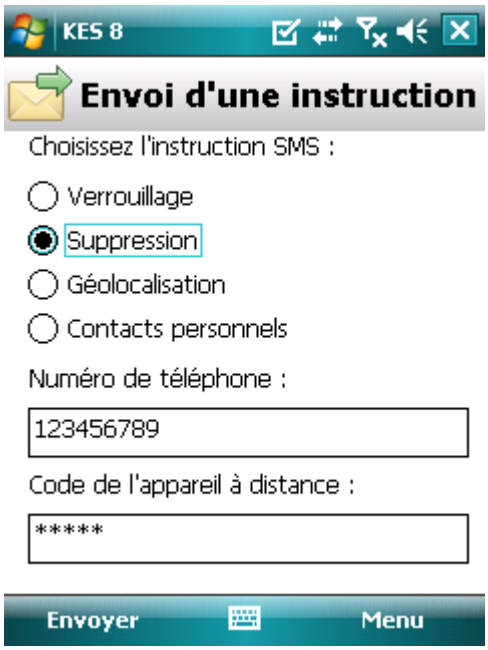

Figure 27: lancement à distance de la fonction Suppression

6. Appuyez sur **Envoyer**.

Pour composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,

envoyez à un autre appareil un SMS contenant le texte `wipe:<code>` (où `<code>` est le code secret défini sur un autre appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES DOSSIERS A SUPPRIMER

La fonction Suppression permet de créer une liste de dossiers qui seront supprimés après la réception de l'instruction SMS spéciale.

Pour qu'Antivol supprime les dossiers de la liste après la réception de l'instruction spéciale par SMS, assurez-vous que la case **Dossiers à supprimer** est cochée dans le menu **Mode**.

La liste des dossiers à supprimer peut contenir les dossiers, ajoutés par l'administrateur. Ces dossiers ne peuvent pas être supprimés de la liste.

Pour ajouter un dossier à la liste des dossiers à supprimer, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

   L'écran **Suppression de données** s'ouvre.

3. Sélectionnez l'option **Dossiers à supprimer**.

   L'écran **Dossiers à supprimer** s'ouvre.

4. Choisissez l'option **Menu** → **Ajouter** (cf. ill. ci-après).

Figure 28: Composition de la liste des dossiers à supprimer

5. Sélectionnez le dossier requis dans l'arborescence, puis cliquez sur **Sélectionner**.

Le dossier sera ajouté à la liste.

Pour supprimer un dossier de la liste, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

   L'écran **Suppression de données** s'ouvre.

3. Sélectionnez l'option **Dossiers à supprimer**.

   L'écran **Dossiers à supprimer** s'ouvre.

4. Sélectionnez un dossier dans la liste, puis appuyez sur **Menu** → **Supprimer**.

CONTROLE DU REMPLACEMENT DE LA CARTE SIM SUR L'APPAREIL

SIM-Surveillance permet, en cas de remplacement de la carte SIM, d'envoyer le nouveau numéro de téléphone au numéro et/ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil.

Pour activer la fonction SIM-Surveillance et contrôler le remplacement de la carte SIM sur l'appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **SIM-Surveillance**.

   L'écran **SIM-Surveillance** s'ouvre.

3. Cochez la case **Activer SIM-Surveillance**.

4. Pour contrôler le remplacement de la carte SIM sur l'appareil, configurez les paramètres suivants (cf. ill. ci-dessous) :

   - Pour recevoir automatiquement un SMS indiquant le nouveau numéro de téléphone de votre appareil, saisissez dans le groupe **Au remplacement de la carte SIM** dans le champ **SMS au numéro de téléphone** le numéro de téléphone vers lequel le SMS sera envoyé.

     Ces numéros peuvent commencer par un chiffre ou par le signe “+» et ne peuvent contenir que des chiffres.

   - Pour recevoir un message électronique indiquant le nouveau numéro de téléphone de votre appareil, saisissez dans le groupe **Au remplacement de la carte SIM** dans le champ **Mess. à l’adresse du courrier élec.** une adresse électronique.

   - Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, cochez dans le groupe **Avancé** la case **Verrouiller l'appareil**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret de l'application.

   - Pour qu'un message apparaisse à l'écran de l'appareil verrouillé, saisissez le texte dans le champ **Texte en cas de verrouillage**. Un texte standard est utilisé par défaut dans ce message. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

Figure 29: paramètres de la fonction SIM-Surveillance

5. Appuyez sur **OK** pour enregistrer les modifications.

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

Après avoir reçu l'instruction spéciale par SMS, la fonction Géolocalisation détermine les coordonnées géographiques de l'appareil et les envoie par SMS ou courrier électronique à l'appareil à l'origine de la demande.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. Le récepteur GPS est activé automatiquement après la réception de l'instruction SMS spéciale. Si l'appareil se trouve dans une zone couverte par satellite, la fonction Géolocalisation reçoit et envoie les coordonnées de l'appareil. Au cas où les satellites ne seraient pas disponibles au moment de la requête, des tentatives pour les trouver sont lancées par la Géolocalisation à intervalles réguliers.

Pour activer la fonction Géolocalisation, procédez comme suit :

1. Choisissez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Sélectionnez l'option **Géolocalisation**.

   L'écran **Géolocalisation** s'ouvre.

3. Cochez la case **Activer la Géolocalisation**.

   Kaspersky Endpoint Security 8 for Smartphone renvoie les coordonnées de l'appareil par SMS.

4. Pour recevoir également les coordonnées par courrier électronique, saisissez dans le groupe **Envoyer les coordonnées de l'appareil** pour le paramètre **Message à l'adresse électronique** l'adresse électronique (cf. ill. ci-après).

Figure 30: paramètres de la fonction Géolocalisation

5. Appuyez sur **OK** pour enregistrer les modifications.

Pour récupérer les coordonnées de l'appareil, si la fonction Géolocalisation est activée, vous disposez des méthodes suivantes :

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS, et l'application enverra les coordonnées de l'appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra un SMS et l'application enverra les coordonnées de l'appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour déterminer les coordonnées de l'appareil, il est conseillé d'utiliser la méthode sûre qui implique la fonction Envoi d'une instruction. Dans ce cas, le code secret sera envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Choisissez l'instruction SMS** la valeur **Géolocalisation** (cf. ill. ci-après).
4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
5. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

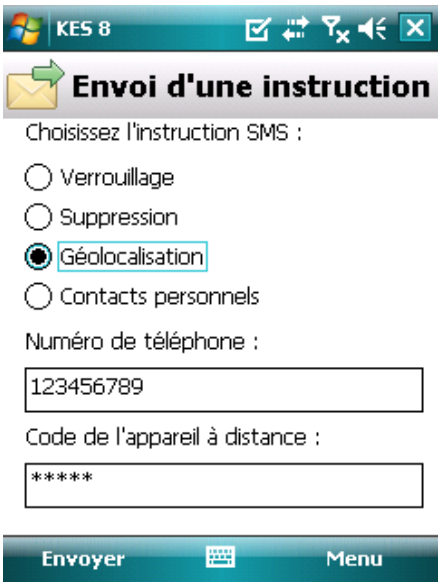

Figure 31: Lancement de la fonction Géolocalisation à distance

6. Appuyez sur **Envoyer**.

Pour composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,

envoyez à un autre appareil un SMS contenant le texte `find:<code>`, où `<code>` est le code secret de l'application défini sur l'autre appareil. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Le SMS contenant les coordonnées géographiques de l'appareil sera envoyé au numéro de téléphone à l'origine de l'envoi de l'instruction SMS et à une adresse électronique, si celle-ci a été définie dans les paramètres de la fonction Géolocalisation.

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

L'application permet d'envoyer une instruction spéciale par SMS afin de lancer à distance la fonction Antivol sur l'autre appareil doté de Kaspersky Endpoint Security 8 for Smartphone. L'instruction SMS est envoyée sous forme d'un SMS crypté qui contient le code secret de l'application, installée sur l'autre appareil. La réception de l'instruction passera inaperçue sur l'autre appareil.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Pour envoyer une instruction SMS vers un autre appareil, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Sélectionnez la fonction à exécuter à distance. Pour ce faire, sélectionnez une des valeurs proposées du paramètre **Choisissez l'instruction SMS** (cf. ill. ci-après) :

   - Verrouillage ;
   - Suppression ;
   - Géolocalisation ;
   - Contacts personnels (cf. la rubrique “Dissimulation des informations confidentielles» à la page 64).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code de l’appareil à distance**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

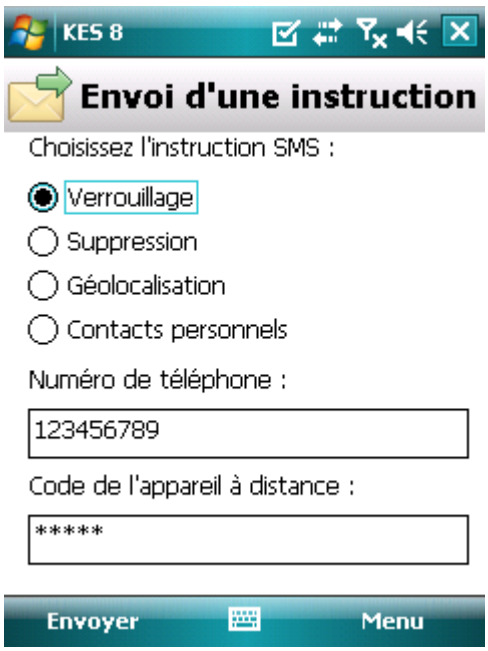

Figure 32: lancement à distance de la fonction Antivol

6. Appuyez sur **Envoyer**.

DISSIMULATION DES INFORMATIONS PERSONNELLES

La section présente le composant Contacts personnels, qui permet de dissimuler les données confidentielles de l'utilisateur.

DANS CETTE SECTION

PRESENTATION DU COMPOSANT CONTACTS PERSONNELS

Les Contacts personnels dissimulent les informations confidentielles sur la base de la Liste de contacts créée qui reprend les numéros confidentiels. Les Contacts personnels masquent les entrées dans les Contacts, les SMS entrants, sortants et brouillons, ainsi que les enregistrements dans le journal des appels pour des numéros confidentiels. Les Contacts personnels bloquent le signal de réception du SMS et le masquent dans la liste des SMS reçus. Les Contacts personnels interdisent les appels entrants d'un numéro confidentiel et l'écran n'indiquera rien au sujet de ces appels. Dans ce cas, la personne qui appelle entendra la tonalité “occupé». Il faut désactiver la dissimulation des informations confidentielles pour pouvoir consulter les appels et les SMS entrants pour la période d'activation de cette fonction. A la réactivation de la dissimulation les informations ne seront pas affichées.

Vous pouvez activer la fonction de dissimulation des informations confidentielles depuis Kaspersky Endpoint Security 8 for Smartphone ou à distance depuis un autre appareil mobile. Vous ne pouvez désactiver la fonction de dissimulation des informations confidentielles que depuis l'application.

Les informations sur le fonctionnement de Contacts personnels sont conservées dans le journal (cf. la rubrique “Journaux de l'application» à la page 86).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

Vous pouvez gérer le mode de fonctionnement de Contacts personnels. Le mode détermine si la fonction de dissimulation des données confidentielles est activée ou non.

Les modes suivants sont prévus pour Contacts personnels :

- **Afficher** : les données confidentielles sont affichées. Les paramètres de Contacts personnels peuvent être modifiés.
- **Masquer** : les données confidentielles sont masquées. Les paramètres du composant Contacts personnels ne peuvent être modifiés.

Vous pouvez configurer l'activation automatique de la dissimulation des données personnelles (à la page 65) ou son activation à distance depuis un autre appareil (cf. rubrique “Activation de la dissimulation des informations confidentielles à distance» à la page 67).

L'état actuel de dissimulation des informations confidentielles figure sur l'écran **Contacts personnels** à côté de l'option de menu **Mode**.

La modification du mode de fonctionnement du composant Contacts personnels peut prendre un certain temps.

ACTIVATION/DESACTIVATION DE CONTACTS PERSONNELS

Vous pouvez modifier le mode de Contacts personnels d'une des méthodes suivantes :

- depuis le menu Contacts personnels ;
- depuis le menu **Contacts personnels**.

Pour modifier le mode de Contacts personnels, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.
2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.
3. Attribuez une valeur au paramètre **Mode Contacts pers.** (cf. ill. ci-après).
4. Appuyez sur **OK**.

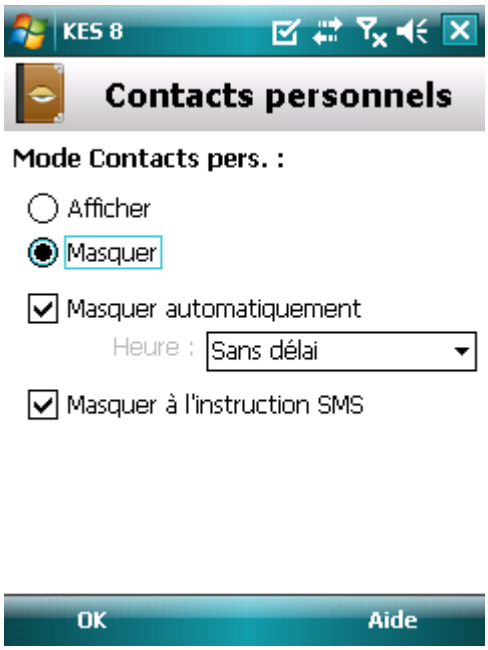

Figure 33: modification du mode de Contacts personnels

5. Confirmez la modification du mode Contacts personnels. Pour ce faire, cliquez sur **Oui**.

Pour changer rapidement le mode Contacts personnels, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.
2. Appuyez sur **Masquer**/**Afficher**. Le texte de l'option change en fonction de l'état actuel de Contacts personnels.
3. Confirmez la modification du mode Contacts personnels. Pour ce faire, cliquez sur **Oui**.

ACTIVATION AUTOMATIQUE DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES

Vous pouvez configurer l'activation automatique de la dissimulation des informations confidentielles après un certain temps. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Désactivez la dissimulation des informations confidentielles avant de modifier les paramètres des Contacts personnels.

Pour activer automatiquement la dissimulation des informations confidentielles à l'issue d'une période déterminée, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Mode**.
3. L'écran **Mode** s'ouvre.
4. Cochez la case **Masquer automatiquement** (cf. ill. ci-après).
5. Sélectionnez la période à l'issue de laquelle la dissimulation des données personnelles doit être activée automatiquement. Pour ce faire, choisissez une des valeurs prédéfinies pour le paramètre **Heure** :
   - **Sans délai** ;
   - **1 minute** ;
   - **5 minutes** ;
   - **15 minutes** ;
   - **1 heure**.

Figure 34: Programmation de la dissimulation automatique des informations confidentielles

6. Appuyez sur **OK**.

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

Kaspersky Endpoint Security 8 for Smartphone permet d'activer à distance la dissimulation des informations confidentielles depuis un autre appareil mobile. Pour ce faire, il faut d'abord activer sur votre appareil la fonction **Masquer par instruction SMS**.

Pour autoriser l'activation à distance de la dissimulation des informations confidentielles, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Cochez la case **Masquer à l'instruction SMS** (cf. ill. ci-après).

Figure 35: Paramètres de la dissimulation des informations confidentielles à distance

4. Appuyez sur **OK**.

Vous pouvez activer à distance la dissimulation des informations confidentielles d'une des méthodes suivantes :

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS qui déclenchera la dissimulation des informations confidentielles. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra un SMS qui déclenchera la dissimulation des informations confidentielles.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile du portable utilisé pour envoyer ce SMS.

Pour activer à distance depuis un autre appareil mobile la dissimulation des informations confidentielles à l'aide d'une instruction SMS spéciale, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Choisissez l'instruction SMS** la valeur **Contacts personnels** (cf. ill. ci-après).
4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
5. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'application, spécifié sur l'appareil destinataire de l'instruction SMS.

Figure 36: Activation de la dissimulation des informations confidentielles à distance

6. Appuyez sur **Envoyer**.

A la réception de l'instruction SMS, la dissimulation des informations confidentielles est activée automatiquement.

Pour activer à distance la dissimulation des informations confidentielles avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à un autre appareil un SMS contenant le texte `hide:<code>` (où `<code>` est le code secret de l'application défini sur un autre appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES NUMEROS CONFIDENTIELS

La liste des contacts contient les numéros confidentiels dont les informations et les événements sont masqués par le composant Contacts personnels. La liste des numéros peut être enrichie manuellement, via importation depuis les contacts ou depuis la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

DANS CETTE SECTION

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez ajouter un numéro dans la Liste des contacts manuellement (par exemple, +12345678) ou l'importer depuis les Contacts ou depuis la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Pour ajouter un numéro de téléphone à la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

3. Exécutez une des opérations suivantes (cf. ill. ci-après) :

   - Pour ajouter un numéro depuis les Contacts, sélectionnez **Menu** → **Ajouter** → **Contact Outlook**. Dans l'écran **Contact Outlook** qui s'ouvre, choisissez l'entrée requise, puis appuyez sur **Sélectionner**.
   - Pour ajouter un numéro enregistré sur la carte SIM, sélectionnez **Menu** → **Ajouter** → **Contact de la carte SIM**. Dans l'écran **Contact de la carte SIM** qui apparaît, sélectionnez l'entrée requise, puis cliquez sur **Sélect**.
   - Pour ajouter un numéro manuellement, choisissez l'option **Menu** → **Ajouter** → **Numéro**. Dans l'écran **Ajouter** qui apparaît, remplissez le champ **Numéro de téléphone** puis cliquez sur **OK**.

Figure 37: ajout d'un enregistrement à la liste des contacts protégés

Le numéro est alors ajouté à la liste des contacts.

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Seuls les numéros qui ont été saisis manuellement dans la Liste des contacts peuvent être modifiés. Il est impossible de modifier les numéros sélectionnés dans le répertoire ou dans la liste des numéros de la carte SIM.

Pour modifier le numéro dans la Liste de contacts, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.
2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.
3. Sélectionnez le numéro à modifier dans la Liste de contacts, puis choisissez **Fonctions** → **Modifier**.

   L'écran **Modifier** s'ouvre.
4. Modifiez les données dans le champ **Numéro de téléphone**.
5. Appuyez sur **OK** une fois les modifications terminées.

Le numéro sera modifié

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez supprimer un numéro de la liste des numéros confidentiels ou purger la Liste de contacts.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Pour supprimer un numéro de la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.
2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.
3. Sélectionnez le numéro à supprimer, puis choisissez **Menu** → **Supprimer**.
4. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

Pour purger la Liste de contacts, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.
2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.
3. Sélectionnez l'option **Menu** → **Supprimer tout**.
4. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

Les Contacts personnels permettent de dissimuler les informations suivantes pour les numéros de la Liste des contacts : contacts, SMS, entrées du journal des appels, SMS et appels entrants. Vous pouvez choisir les informations et les événements que la fonction Contacts personnels va dissimuler pour les numéros confidentiels.

Désactivez la dissimulation des informations confidentielles avant de modifier les paramètres des Contacts personnels.

Pour choisir les informations et les événements à masquer pour les numéros confidentiels, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Choisissez l'option **Objets à masquer**.

   L'écran **Objets à masquer** (cf. ill. ci-après) apparaît.

3. Dans le groupe **Masquer les entrées**, choisissez les informations qui seront dissimulées pour les numéros confidentiels. Les paramètres suivants sont prévus:

   - **Contacts :** masque toutes les informations relatives aux numéros confidentiels.
   - **SMS** : masque les SMS dans les dossiers **Boîte de réception**, **Messages envoyés**, **Brouillons** pour les numéros confidentiels.
   - **Appels** : accepte les appels en provenance des numéros confidentiels mais ne définit pas le numéro de l'appelant et n'affiche pas les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).

4. Dans le groupe **Masquer les événements**, sélectionnez les événements qui seront masqués pour les numéros confidentiels. Les paramètres suivants sont prévus:

   - **SMS entrants** : masquer la réception de SMS entrants (rien n'indiquera à l'écran qu'un SMS en provenance d'un numéro confidentiel vient d'arriver). Tous les SMS envoyés depuis les numéros confidentiels pourront être consultés lorsque la dissimulation des informations confidentielles sera désactivée.
   - **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité “occupé»). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.

Figure 38: sélection des informations et des événements à dissimuler

5. Appuyez sur **OK**.

FILTRAGE DE L'ACTIVITE DE RESEAU PARE-FEU

La section présente le composant Pare-feu, qui contrôle les connexions de réseau sur votre appareil. De plus, elle décrit comment activer / désactiver le composant Pare-feu et comment sélectionner le mode de fonctionnement requis.

DANS CETTE SECTION

À PROPOS DU PARE-FEU

Le Pare-feu contrôle les connexions de réseau sur votre appareil selon le mode sélectionné. Pare-feu permet de désigner les connexions autorisées (par exemple, pour synchroniser avec le Serveur d'administration), ainsi que les connexions interdites (par exemple, pour l'utilisation d'Internet et le téléchargement de fichiers).

Pare-feu permet de configurer les notifications des connexions bloquées (cf. la rubrique “Présentation des modes Pare-feu» à la page 73).

Les informations sur le fonctionnement du Pare-feu sont consignées dans le journal de l'application (voir section “Journaux de l'application» à la page 86).

PRESENTATION DES MODES PARE-FEU

Vous pouvez sélectionner le mode Pare-feu pour définir les connexions autorisées et interdites. Les modes de fonctionnement Pare-feu disponibles :

- **Désact.** : autorisation de la moindre activité de réseau.
- **Protection minimum** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Protection maximum** : bloque toutes les connexions entrantes. La réception du courrier, la consultation d'Internet et le téléchargement de fichiers sont autorisés. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Tout bloquer** : bloque toute activité de réseau, sauf la mise à jour des bases antivirus et la connexion au système d'administration distante.

Vous pouvez modifier le mode Pare-feu (cf. la rubrique “Sélection du mode Pare-feu» à la page 73). Le mode actuel est indiqué sur l'écran **Pare-feu** à côté de l'option de menu **Mode**.

SELECTION DU MODE PARE-FEU

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour sélectionner le mode du Pare-feu, procédez comme suit :

1. Sélectionnez **Menu** → **Pare-feu**.

   L'écran **Pare-feu** apparaît.

2. Sélectionnez l'option **Mode**.

   L'écran **Pare-feu** apparaît.

3. Sélectionnez le mode Pare-feu (cf. ill. ci-après).

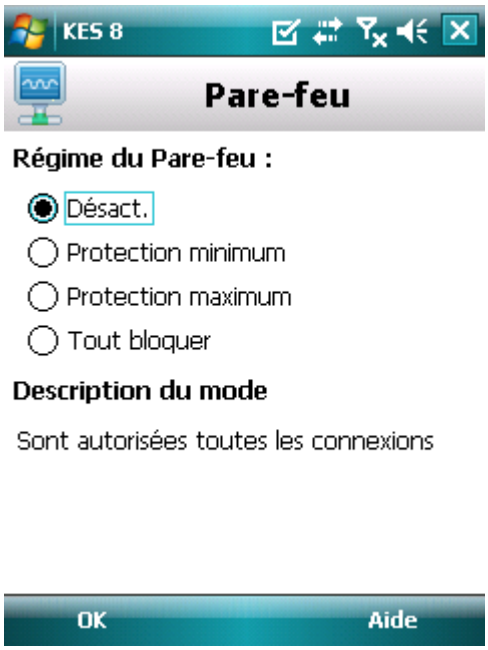

Figure 39: sélection du niveau de sécurité du Pare-feu

4. Appuyez sur **OK**.

NOTIFICATIONS SUR LE BLOCAGE DES CONNEXIONS

Le Pare-feu permet d'obtenir des notifications sur le blocage des connexions. Vous pouvez configurer la réception des notifications Pare-feu.

Pour administrer les notifications sur le blocage, procédez comme suit :

1. Sélectionnez **Menu** → **Pare-feu**.

   L'écran **Pare-feu** apparaît.

2. Choisissez l'option **Notifications**.

   L'écran **Notifications** (cf. ill. ci-après) s'ouvre.

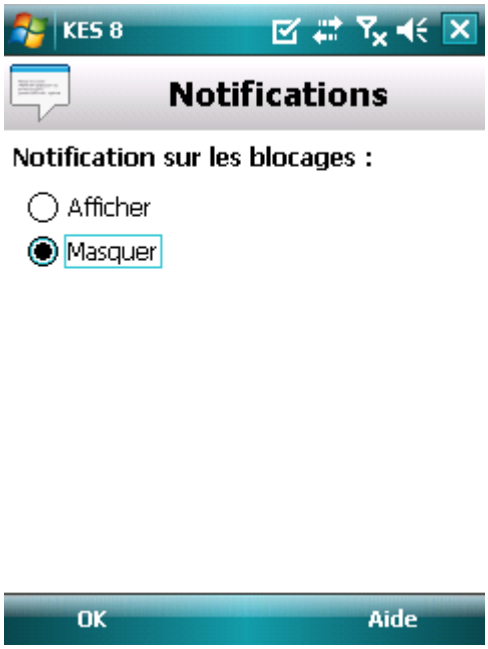

Figure 40 : configuration de la remise des notifications sur le blocage des connexions

3. Dans le groupe **Notifications sur les blocages**, sélectionnez une des options proposées :
   - **Afficher** : active la remise des notifications. Le Pare-feu signale le blocage de la connexion.
   - **Masquer** : désactiver la distribution des notifications. Le Pare-feu ne signale pas le blocage de la connexion.
4. Appuyez sur **OK**.

CHIFFREMENT DES DONNEES PERSONNELLES

La section présente le composant Chiffrement, qui permet de chiffrer les dossiers sur l'appareil. De plus, la section décrit comment chiffrer et déchiffrer les dossiers sélectionnées.

DANS CETTE SECTION

À PROPOS DU CHIFFREMENT

La fonction Chiffrement chiffre les informations de la liste des dossiers à chiffrer que vous avez créée. La fonction Chiffrement repose sur une fonction de cryptage intégrée au système d'exploitation de votre appareil. La fonction Chiffrement permet de chiffrer tous les dossiers, sauf les dossiers système. Vous pouvez sélectionner pour le chiffrement des dossiers stockés dans la mémoire de l'appareil ou sur une carte mémoire. Pour pouvoir accéder aux informations chiffrées, il faut saisir le code secret défini à la première exécution de l'application.

Avant de lancer des fichiers exe exécutables depuis le dossier chiffré, il faut déchiffrer ce dossier. Pour ce faire, saisissez le code secret de l'application.

Pour pouvoir accéder aux informations chiffrées, il faut saisir le code secret de l'application (cf. rubrique “Saisie du code secret» à la page 24). Vous pouvez définir la période (cf. rubrique “Interdiction d'accès aux données chiffrées» à la page 79), à l'issue de laquelle l'interdiction d'accès aux dossiers chiffrés sera activée et un code secret de l'application sera nécessaire pour accéder à ces dossiers. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Les informations sur le fonctionnement du Chiffrement sont consignées dans le journal de l'application (cf. la rubrique “Journaux de l'application» à la page 86).

CHIFFREMENT DES DONNEES

Le Chiffrement permet de chiffrer un nombre quelconque de dossiers non systèmes qui se trouvent dans la mémoire de l'appareil ou sur une carte mémoire.

La liste de tous les dossiers chiffrés ou déchiffrés antérieurement est accessible dans l'écran **Chiffrement** via l'option **Liste des dossiers**.

Vous pouvez également chiffrer un dossier ou chiffrer directement tous les dossiers qui se trouvent dans la liste des dossiers.

Pour ajouter un dossier à la liste des dossiers à chiffrer pour le chiffrer, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

3. Appuyez sur **Menu** → **Ajouter** (cf. ill. ci-après).

Figure 41: sélection du dossier à chiffrer

   L'écran reprenant l'arborescence du système de fichiers de l'appareil apparaît.

4. Sélectionnez le dossier à chiffrer, puis cliquez sur **Chiffrer**.

   Pour parcourir le système de fichiers, utilisez le stylet ou les boutons du joystick de l'appareil.

   Kaspersky Endpoint Security 8 for Smartphone vous préviendra lorsque la procédure de chiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

5. Appuyez sur **OK**.

   Pour le dossier sélectionné, l'option **Chiffrer** du **Menu** devient **Déchiffrer**.

Après le chiffrement, les fichiers sont déchiffrés et chiffrés automatiquement lorsque vous manipulez des fichiers depuis un dossier chiffré, lorsque vous les extrayez du dossier chiffré ou y placer de nouveaux fichiers.

Pour chiffrer directement tous les dossiers de la liste, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

3. Sélectionnez **Menu** → **Actions compl.** → **Tout chiffrer**.

   Kaspersky Endpoint Security 8 for Smartphone vous préviendra lorsque la procédure de chiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

4. Appuyez sur **OK**.

DECHIFFREMENT DES DONNEES

Il est possible de déchiffrer les données préalablement chiffrées (cf. la rubrique “Chiffrement de données» à la page 76) Vous pouvez déchiffrer un seul dossier ou tous les dossiers que vous avez chiffrés sur l'appareil.

Si la liste des dossiers à chiffrer contient les dossiers chiffrés par l'administrateur, vous ne pourrez ni les déchiffrer ni les supprimer de la liste.

Pour déchiffrer un dossier chiffré, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** apparaît. Il reprend la liste de tous les dossiers chiffrés et déchiffrés antérieurement.

3. Sélectionnez le dossier chiffré dans la liste, puis appuyez sur **Menu** → **Déchiffrer** (cf. ill. ci-après).

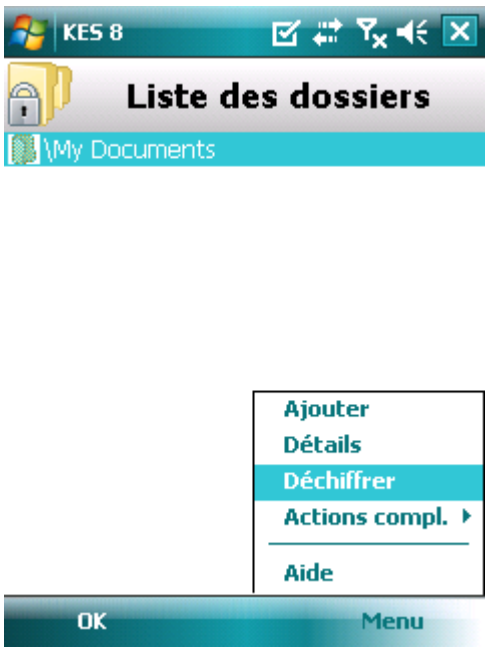

Figure 42: activation de la fonction

   Kaspersky Endpoint Security 8 for Smartphone vous préviendra lorsque la procédure de déchiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

4. Appuyez sur **OK**.

Pour le dossier déchiffré, l'option **Déchiffrer** du **Menu** devient **Chiffrer**. Vous pouvez à nouveau chiffrer un dossier (cf. la rubrique “Chiffrement de données» à la page 76).

Pour déchiffrer directement tous les dossiers de la liste des dossiers à déchiffrer, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

3. Sélectionnez **Menu** → **Actions compl.** → **Tout déchiffrer**.

   Lorsque la procédure de déchiffrement sera terminée, Kaspersky Endpoint Security 8 for Smartphone vous en préviendra par une notification qui s'affichera sur l'écran.

4. Appuyez sur **OK**.

INTERDICTION D'ACCES AUX DONNEES CHIFFREES

Le Chiffrement permet de définir la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée. La fonction est activée au moment de passage de l'appareil en mode d'économie de l'énergie. Pour utiliser les informations chiffrées, il faudra saisir le code secret de l'application.

Pour interdire l'accès à un dossier chiffré à l'issue d'une période déterminée, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Interdiction de l'accès**.

   L'écran **Interdiction de l'accès** s'ouvre

3. Déterminez la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée. Pour ce faire, attribuez au paramètre **Bloquer l'accès** une des valeurs proposées (cf. ill. ci-après) :

   - **Sans délai** ;
   - **1 minute** ;
   - **5 minutes** ;
   - **15 minutes** ;
   - **1 heure**.

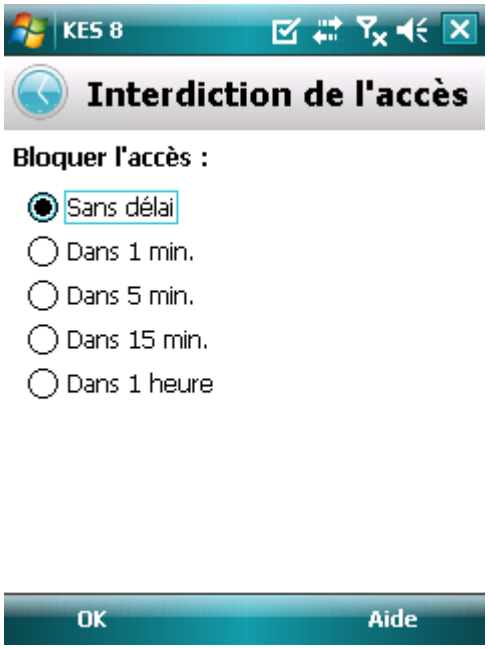

Figure 43: blocage de l'accès aux données chiffrées

4. Appuyez sur **OK** pour enregistrer les modifications.

Pour interdire l'accès aux dossiers chiffrés après leur ouverture,

cliquez sur l'icône de Kaspersky Endpoint Security 8 for Smartphone dans la barre système de l'appareil et sélectionnez **Verrouiller les données** (cf. ill. ci-après). L'interdiction de l'accès aux informations chiffrées sera activée.

Figure 44: menu contextuel de l'application dans la barre d'état système de l'appareil

MISE A JOUR DES BASES DU PROGRAMME

La section présente la mise à jour des bases anti-virus de l'application qui garantit l'actualité de la protection de votre appareil. Elle explique également comment consulter les informations relatives aux bases antivirus installées, comment lancer la mise à jour manuelle ou comment programmer celle-ci.

DANS CETTE SECTION

À PROPOS DE LA MISE A JOUR DES BASES

La recherche d'application malveillante s'opère à l'aide d'une base antivirus qui contient les descriptions de toutes les applications malveillantes connues à ce jour et des moyens de les neutraliser ainsi que des descriptions d'autres objets indésirables. Il est extrêmement important d'assurer la mise à jour des bases antivirus.

Il est conseillé d'actualiser régulièrement les bases de l'application. Si plus de 15 jours se sont écoulés depuis la dernière mise à jour, les bases de l'application sont considérées comme étant fortement dépassées. Dans ce cas, la fiabilité de la protection sera réduite.

Kaspersky Endpoint Security 8 for Smartphone effectue la mise à jour des bases de l'application depuis les serveurs de mises à jour définis par l'administrateur.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur Internet.

La mise à jour des bases antivirus de l'application s'opère selon l'algorithme suivant :

1. Les bases de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour spécial.
2. Kaspersky Endpoint Security 8 for Smartphone exécute une des opérations suivantes :
   - Si les bases de l'application que vous utilisez sont à jour, la mise à jour sera annulée. Un message d'information s'affichera à l'écran.
   - Si les bases installées diffèrent, alors le nouveau paquet de mise à jour sera téléchargé et installé.

     Une fois la mise à jour terminée, la connexion est automatiquement coupée. Si la connexion était déjà établie avant la mise à jour, elle reste alors disponible pour d'autres opérations.

Vous pouvez lancer la tâche de mise à jour manuellement à n'importe quel moment, si l'appareil n'est pas occupé par l'exécution d'autres tâches ou programmer l'exécution de la mise à jour.

Vous pouvez obtenir des informations détaillées sur les bases utilisées sur l'écran **Mises à jour** via le point **Infos des bases**.

Les informations sur la mise à jour des bases antivirus sont consignées dans le journal de l'application (cf. la rubrique “Journaux de l'application» à la page 86).

AFFICHAGE D'INFORMATIONS SUR LES BASES

Vous pouvez consulter les informations sur les bases antivirus de l'application installées : dernier lancement de la mise à jour, date de publication des bases, taille des bases et nombre d'entrées dans les bases.

Pour consulter les informations sur les bases antivirus existantes, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Choisissez l'option **Infos des bases**.

   L'écran **Infos des bases** s'ouvre. Il présente des informations sur les bases antivirus de l'application installées (cf. ill. ci-après).

Figure 45: informations relatives aux bases antivirus de l'application installées

MISE A JOUR MANUELLE

Vous pouvez lancer manuellement la mise à jour des bases antivirus de l'application.

Pour lancer la mise à jour manuelle des bases antivirus de l'application, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Mise à jour** (cf. ill. ci-après).

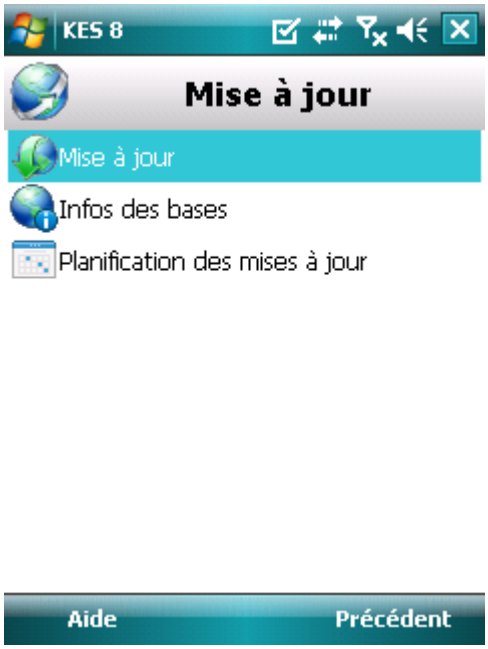

Figure 46: lancement manuel de la mise à jour

L'application lance la mise à jour des bases antivirus depuis le serveur, défini par l'administrateur. Les informations sur la mise à jour apparaissent à l'écran.

LANCEMENT PROGRAMME DE LA MISE A JOUR

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Pour votre confort, vous pouvez configurer l'exécution automatique de la mise à jour des bases antivirus et de programmer son exécution.

Pour exécuter une mise à jour programmée, veillez à ce que l'appareil soit allumé au moment de la mise à jour.

Pour configurer le lancement programmé de la mise à jour, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Planification des MAJ**.

   L'écran **Programmation** s'ouvre.

4. Cochez la case **Mise à jour programmée** (cf. ill. ci-après).

5. Programmez l'exécution de la mise à jour. Pour ce faire, attribuez une valeur au paramètre **Fréquence** :

   - **Chaque jour** : actualise les bases chaque jour. Saisissez la valeur pour le paramètre **Heure**.
   - **Chaque semaine** : actualise les bases de l'application une fois par semaine. Sélectionnez une valeur pour les paramètres **Heure** et **Jour de la semaine**.

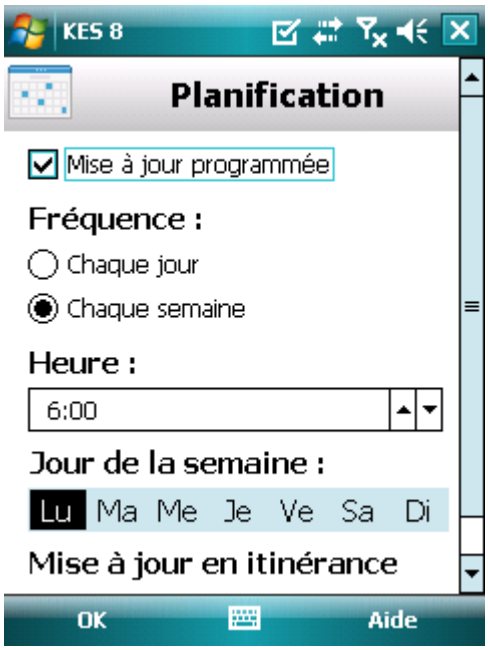

Figure 47: Paramètres de lancement planifié de la mise à jour

6. Appuyez sur **OK** pour enregistrer les modifications.

MISE A JOUR EN ITINERANCE

Vous pouvez contrôler le lancement programmé de la mise à jour en itinérance, vu que le trafic internet est payé au tarif d'itinérance.

Si le lancement programmé de la mise à jour est interdit en itinérance, le lancement manuel de la mise à jour sera accessible en mode normal.

Pour interdire la mise à jour programmée en cas d'itinérance, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Planification des MAJ**.

   L'écran **Programmation** s'ouvre.

4. Dans le groupe **Mise à jour en itinérance**, décochez la case **Mettre à jour en itinérance**.

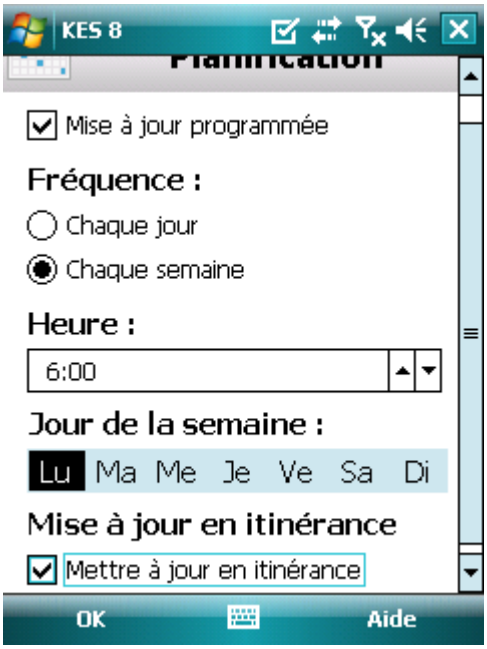

Figure 48: Paramètres de lancement de la mise à jour automatique en itinérance

5. Appuyez sur **OK** pour enregistrer les modifications.

JOURNAUX DU LOGICIEL

La section présente des informations sur les journaux où sont consignées les informations sur le fonctionnement de chaque composant ainsi que les informations sur l'exécution de chaque tâche (par exemple, mise à jour des bases antivirus de l'application, analyse antivirus)

DANS CETTE SECTION

À PROPOS DES JOURNAUX

Les journaux reprennent les rapports sur les événements survenus pendant le fonctionnement de chaque composant de Kaspersky Endpoint Security 8 for Smartphone. Il existe un journal des événements pour chaque composant. Vous pouvez sélectionner et consulter le rapport sur les événements survenus pendant l'utilisation du composant. Les entrées du rapport sont classées dans l'ordre chronologique décroissant.

AFFICHAGE DES EVENEMENTS DU JOURNAL

- *Pour consulter tous les enregistrements repris dans le journal, procédez comme suit :*

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Journaux**.

   L'écran **Journal Anti-Virus** s'ouvre.

3. Choisissez le composant pour lequel vous souhaitez consulter le journal.

Le journal du composant sélectionné s'ouvre (cf. ill. ci-après).

Figure 49 : Affichage d'événements dans les journaux

- *Pour afficher des informations détaillées sur les enregistrements du journal,*

  sélectionnez l'enregistrement requis puis cliquez sur **Détails**.

  L'écran **Détails** reprend les informations sur l'action exécutée par l'application en détail. Par exemple, pour l'action “Objet en quarantaine», le chemin d'accès au fichier infecté sur l'appareil est également affiché.

- *Pour revenir à la liste des journaux,*

  appuyez sur **Menu** → **Précédent**.

SUPPRESSION DES ENREGISTREMENTS DU JOURNAL

Vous pouvez purger tous les journaux. Les informations relatives au fonctionnement des composants de Kaspersky Endpoint Security 8 for Smartphone seront supprimées.

Pour purger tous les journaux, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Journaux**.

   L'écran **Journal Anti-Virus** s'ouvre

3. Ouvrez le journal de n'importe quel composant.
4. Sélectionnez l'option **Menu** → **Supprimer tout**.
5. Pour confirmer la suppression, cliquez sur **Oui**.

Tous les événements du journal de chaque composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section présente les possibilités complémentaires de Kaspersky Endpoint Security 8 for Smartphone : comment modifier le code secret de l'application, comment administrer les notifications sonores de l'application et comment activer / désactiver l'affichage des astuces avant la configuration des paramètres de chaque composant.

DANS CETTE SECTION

MODIFICATION DU CODE SECRET

Vous pouvez modifier le code secret de l'application, défini à la première exécution de l'application.

Pour changer le code secret de l'application, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

3. Choisissez l'option **Modification du code**.

4. Saisissez le code secret actuel de l'application dans la zone **Saisissez le code**.

5. Saisissez le nouveau code secret de l'application dans le champ **Saisissez le nouveau code** et dans le champ **Confirmation du code**, puis cliquez sur **OK** pour conserver les modifications.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des composants, Kaspersky Endpoint Security 8 for Smartphone affiche par défaut des astuces reprenant une brève description de la fonction sélectionnée. Vous pouvez configurer l'affichage des astuces de Kaspersky Endpoint Security 8 for Smartphone.

Pour configurer l'affichage des astuces, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

3. Sélectionnez l'option **Astuces**.

   L'écran **Astuces** s'ouvre.

4. Sélectionnez une des valeurs proposées pour le paramètre **Astuces** :

   - **Afficher** : affiche l'astuce avant de configurer les paramètres de la fonction sélectionnée.
   - **Masquer** : aucune astuce n'est affichée.

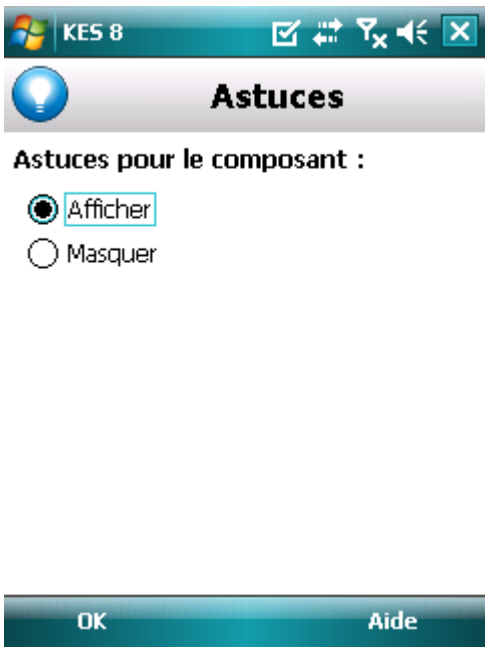

Figure 50: configuration de l'affichage des astuces

5. Appuyez sur **OK**.

ADMINISTRATION DES NOTIFICATIONS SONORES

De différents événements résultent de l'exécution de l'application, par exemple, découverte d'un objet infecté ou d'un virus, expiration de la licence. Pour que l'application vous signale chacun de ces événements, vous pouvez activer la notification sonore pour les événements survenus.

Kaspersky Endpoint Security 8 for Smartphone active la notification sonore uniquement selon le mode défini de l'appareil.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour administrer les notifications sonores de l'application, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

3. Choisissez l'option **Son**.

   L'écran **Son** s'ouvre.

4. Sélectionnez une des valeurs proposées pour le paramètre **Notifications sonores** (cf. ill. ci-après) :

   - **Activer** : utilise les notifications sonores quel que soit le profil sélectionné pour l'appareil.
   - **Désactiver** : n'utilise pas les notifications sonores.

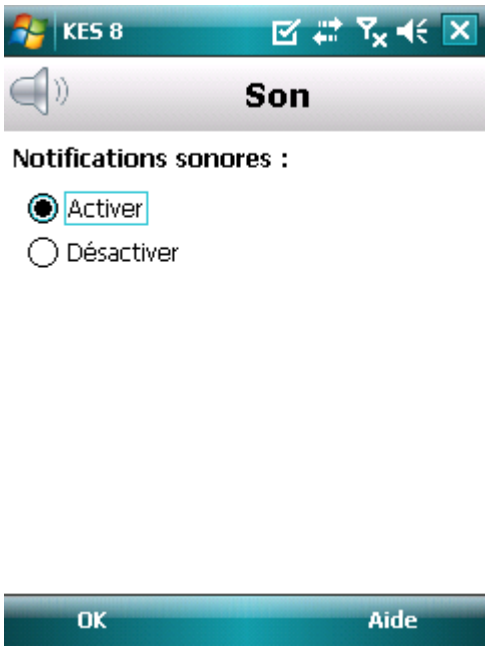

Figure 51 : Configuration des notifications sonores

5. Appuyez sur **OK** pour enregistrer les modifications.

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'application ne peut être activée qu'avec une licence installée.

ANALYSE A LA DEMANDE

Mode de fonctionnement du programme Kaspersky Lab exécuté à la demande de l'utilisateur et conçu pour analyser et vérifier tous les fichiers résidents.

ARCHIVE

Fichier “conteneur» d'un ou plusieurs autres objets pouvant être eux-mêmes des archives.

B

BASES ANTIVIRUS

Bases de données maintenues par les experts de Kaspersky Lab contenant des descriptions détaillées de toutes les menaces de sécurité informatique existantes, ainsi que les méthodes permettant de les détecter et de les neutraliser. La base de données est constamment mise à jour par Kaspersky Lab chaque fois qu'une nouvelle menace apparaît.

BLOCAGE D'UN OBJET

Interdire l'accès à un objet par des programmes externes. Un objet interdit ne peut pas être lu, exécuté, modifié ni supprimé.

C

CODE SECRET DE L'APPLICATION

Le code secret de l'application permet d'éviter l'accès non autorisé aux paramètres de l'application et aux données protégées de l'appareil. Il est saisi par l'utilisateur à la première exécution de l'application et compte au moins quatre chiffres. Il faut saisir le code secret de l'application dans les cas suivants :

- Pour accéder aux paramètres de l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Géolocalisation, Contacts personnels ;
- Pour supprimer l'application.

D

DESINFECTION OU REPARATION D'OBJETS

Méthode de traitement d'objets infectés permettant la récupération complète ou partielle des données, ou la prise d'une décision si l'objet ne peut être réparé. La réparation d'objets fait appel au contenu des bases de données. La réparation peut entraîner la perte d'une partie des données.

L

LISTE BLANCHE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par l'Anti-Spam.

- Type d'événement en provenance de ce numéro que l'Anti-Spam accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à l'Anti-Spam d'identifier des SMS sollicités (qui ne sont pas du spam). L'Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

LISTE NOIRE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par l'Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Anti-Spam bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à l'Anti-Spam d'identifier des SMS non sollicités (spam). L'Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

M

MASQUE DU NUMERO DE TELEPHONE

Présentation du numéro de téléphone dans la liste noire ou blanche par les caractères communs. Les deux caractères génériques de base utilisés dans les masques de numéro de téléphone sont “*» et “?» (où * représente une suite de caractères quelconques et ? un seul caractère). Il s'agit, par exemple, du numéro *1234 ? de la Liste noire. L'Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de maintenir la protection à jour. Elle copie les bases antivirus depuis les serveurs de mises à jour de Kaspersky Lab sur l'appareil en les intégrant à l'application en mode automatique.

N

NON-NUMERIQUES

Numéro de téléphone contenant des lettres ou composé intégralement de lettres.

O

OBJET INFECTE.

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible car une section du code de l'objet est identique à la section de code d'une menace déjà connue. Les experts de Kaspersky Lab ne recommandent pas d'utiliser des objets de ce type, qui peuvent causer l'infection de l’appareil.

P

PLACER DES OBJETS EN QUARANTAINE

Méthode permettant de traiter des objets probablement infectés, en interdisant leur accès et en les déplaçant de leur position d'origine vers le dossier de quarantaine, où l'objet est enregistré sous une forme chiffrée qui annule toute menace d'infection.

Q

QUARANTAINE.

Dossier spécial dans lequel sont placés tous les objets probablement infectés, détectés pendant l'analyse de l’appareil ou par la protection en temps réel.

R

RESTAURATION

Restitution de l'objet en quarantaine ou sauvegardé dans le dossier d'origine où il se trouvait avant d'être placé en quarantaine ou réparé, ou bien encore, dans un autre dossier choisi par l'utilisateur.

S

SUPPRESSION SMS

Méthode de traitement d'un SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des messages SMS clairement indésirables.

SUPPRESSION D'UN OBJET

Procédé de traitement d'un objet, impliquant sa suppression physique de l'emplacement où il a été détecté par le programme (disque fixe, dossier, ressource réseau). Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

SYNCHRONISATION

Un processus d'établissement de la connexion entre l'appareil mobile et le système d'administration distante suivi de la transmission des données. Lors de la synchronisation, l'appareil reçois les paramètres de l'application, installés par l'administrateur. L'appareil envoie dans le système d'administration distante les rapports sur le fonctionnement des composants de l'application.

SYSTEME D'ADMINISTRATION DISTANTE

Un système qui permet de contrôler les appareils à distance et de les administrer en temps réel.

KASPERSKY LAB ZAO

Fondé en 1997, Kaspersky Lab Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches Anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes seniors de Kaspersky Lab sont membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, soutenues par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse approfondie de l'activité virale informatique permet aux spécialistes de la société de détecter les tendances dans l'évolution du code malveillant et d'offrir à nos utilisateurs une protection permanente contre les nouveaux types d'attaques. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour assurer la plus grande des protections anti-virus aussi bien aux particuliers, qu'aux clients corporatifs.

Des années de dur travail ont fait de notre société l'un des premiers fabricants de logiciels antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Anti-Virus : il assure une protection complète de tous les systèmes informatiques contre les attaques de virus, comprenant les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nous assurons l'étude, l'installation et la maintenance de suites antivirus de grandes organisations. La base anti-virus de Kaspersky Lab est mise à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
L'Encyclopédie des virus:	http://www.securelist.com/fr
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)

UTILISATION DE CODE TIERS

Le code développé par d'autres éditeurs a été utilisé pour créer l'application.

La bibliothèque logicielle de protection des informations (BLPI) Crypto C, développée par CryptoEx intervient dans la formation et la vérification de la signature numérique.

Le site de CryptoEx : http://www.cryptoex.ru.

INDEX

A

B

C

D

E

F

I

J

K

L

M

N

P

Q

R

S

V